Configuring SNMP, RMON, BOOTP, DHCP, and RARP Services

Router Software Version 11.01
Site Manager Software Version 5.01

Part No. 114070 Rev. B
February 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1997 Bay Networks, Inc.

All rights reserved. Printed in the USA. February 1997.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, Bay Networks, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and ANH, ASN, Bay•SIS, BayStack, BayStream, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

About This Guide

Before You Begin xvi
Conventions xvi
Acronyms xvii
Ordering Bay Networks Publications xviii

Technical Support and Online Services

Bay Networks Customer Service xx
Bay Networks Information Services xxi
World Wide Web xxi
Customer Service FTP xxi
Support Source CD xxii
CompuServe xxii
InfoFACTS xxiii
How to Get Help xxiii

Chapter 1
Starting SNMP, RMON, BOOTP, DHCP, and RARP Services

Before You Begin 1-1
Starting SNMP Services 1-2
Enabling IP on an Interface 1-2
Customizing IP 1-3
Starting RMON 1-3
Enabling the Ethernet DCM 1-4
Customizing the Ethernet DCM 1-4
Starting BOOTP Services 1-5
Enabling BOOTP on an Interface 1-5
Customizing BOOTP 1-5
Starting DHCP 1-6
Enabling DHCP on an Interface 1-6

Customizing DHCP 1-7
Starting RARP Services 1-7
Enabling RARP on an Interface 1-7
Customizing RARP 1-8

Chapter 2
SNMP, RMON, BOOTP, DHCP, and RARP Concepts

SNMP Overview 2-1
SNMP Messages 2-2
SNMP Communities 2-4
SNMP Implementation Notes 2-4
Internet Protocol (IP) 2-5
Events and Traps 2-5
Protocol Entities 2-5
Severity Levels 2-6
SNMP Trap Format 2-6
Thresholds 2-7
Threshold Example 2-8
Event Message Format 2-9
State of a Threshold 2-9
Memory Considerations 2-9
RMON Overview 2-10
How RMON Works 2-10
RMON Architecture 2-12
RMON MIB Groups 2-13
Statistics Group 2-13
History Group 2-14
Host Group 2-14
HostTopN Group 2-14
Matrix Group 2-14
Filter Group 2-14
Capture Group 2-15
Alarm Group 2-15
Event Group 2-16
RMON Interoperability Issues 2-17
RMON Applications 2-18

RMON Memory Use 2-18
Interoperability Issues and Memory Use for RMON Groups 2-19
Statistics Group 2-19
History Group 2-20
Host Group 2-20
HostTopN Group 2-21
Matrix Group 2-22
Filter and Capture Groups 2-22
Alarm and Event Groups 2-24
BOOTP Relay Agent Overview 2-24
DHCP Overview 2-29
Acquiring a New IP Address and New Configuration Parameters 2-30
Acquiring the Same IP Address Again 2-34
RARP Overview 2-35

Chapter 3
Customizing SNMP

Customizing SNMP Global Parameters 3-1
Disabling and Reenabling SNMP 3-1
Enabling and Disabling SNMP Locking 3-2
Specifying a Lock Timeout Period 3-2
Enabling and Disabling Authentication Failure Traps 3-3
Configuring SNMP Community Parameters 3-3
Adding an SNMP Community 3-3
Specifying a Community Name 3-3
Specifying Community Access Privileges 3-4
Deleting an SNMP Community 3-4
Configuring SNMP Community Managers 3-5
Adding a Manager 3-5
Configuring a Manager to Receive Traps 3-6
Specifying the Trap Port 3-6
Specifying a Trap Type 3-6
Deleting a Manager 3-7
Configuring Traps on the Router 3-7
Specifying a Trap Entity and Severity Level 3-8
Configuring Trap Exceptions 3-9

Deleting Trap Exceptions 3-10
Configuring Thresholds 3-10
Disabling and Reenabling Thresholds 3-10
Setting the Threshold Polling Interval 3-11
Adding a Threshold 3-11
Enabling and Disabling Thresholds for a Variable 3-12
Specifying a Value for the Threshold Level 3-12
Specifying the Severity Level for Event Messages 3-12
Specifying Threshold Units 3-13
Determining When to Record Threshold Events 3-13
Specifying Maximum Successive Alarms 3-13
Specifying Polling Intervals for Held Variables 3-14
Specifying a Threshold Object Name 3-14

Chapter 4
Customizing a DCM for RMON

Ethernet DCM and RMON Summary 4-1
Modifying the DCM Configuration 4-2
Specifying the DCM Boot Image Name 4-2
Specifying the Boot Option 4-3
Saving the Boot Image File 4-3
Specifying the Configuration Mode 4-3
Saving the Configuration Information 4-4
Specifying the Maximum Number of RMON Hosts 4-4
Disabling the RMON Host Control Table 4-4
Disabling the RMON Default Matrix Table 4-5
Rebooting the Ethernet DCM 4-5
Deleting the Ethernet DCM Software Subsystem 4-5
Managing a DCM Using the Technician Interface 4-6
Viewing and Analyzing Statistics Using Optivity 4-7
Using Optivity Analysis with RMON 4-7
Using Optivity LAN with RMON 4-10
Threshold Manager Tool 4-10
Fault Correlator Tool 4-11

Chapter 5
Customizing BOOTP

Customizing BOOTP Relay Agent Parameters 5-1
Disabling and Reenabling BOOTP 5-1
Specifying Maximum Number of Hops from Client to Server 5-2
Specifying a Minimum Timeout Value 5-2
Filtering Unwanted BOOTP and DHCP Packets 5-2
Setting Up the Routing Path between the BOOTP Server and the Routers 5-3
Enabling BOOTP on Router Interfaces 5-3
Specifying Interfaces to Receive and Relay BOOTREQUEST Packets 5-5
Creating a BOOTP Relay Agent Forwarding Table 5-5
Specifying the IP Interface Input/Output Address Pair 5-5
Deleting an IP Interface Input/Output Address Pair 5-6
Disabling BOOTP Route Forwarding 5-6
Configuring an AN to Use EZ-Install over a Frame Relay PVC 5-7
Creating a BOOTP Client Interface Table 5-7
Specifying the Client IP Address 5-7
Specifying the DLCI Number 5-8
Specifying Servers for BOOTP Services 5-8
Configuring BOOTP Preferred Servers 5-8
Specifying the Relay Agent IP Address 5-8
Specifying the Target Server IP Address 5-9
Specifying the Target Server's Host Name 5-9
Disabling the Forwarding Route 5-9
Filtering BOOTP and DHCP Packets 5-9
Deleting the BOOTP Relay Agent from an IP Interface 5-10
Deleting BOOTP Globally 5-10

Chapter 6
Customizing DHCP

Customizing DHCP Parameters 6-1
Specifying Interfaces to Receive and Relay DHCP Packets 6-1
Specifying Servers for DHCP Services 6-2
Deleting DHCP from an IP Interface 6-2
Deleting DHCP Globally 6-2

Chapter 7
Customizing RARP

Customizing RARP Parameters 7-1
Disabling and Reenabling RARP Interfaces 7-1
Defining the RARP Mapping Table 7-2
Specifying the Client's MAC Address 7-2
Specifying the Client's IP Address 7-2
Disabling RARP Globally 7-3
Deleting RARP Globally 7-3

Appendix A
SNMP, DCM, BOOTP, DHCP, and RARP Parameter Descriptions

SNMP Global Parameters A-2
SNMP Community Parameters A-4
SNMP Manager Parameters A-5
SNMP Trap Interface Parameters A-6
SNMP Threshold Global Parameters A-7
SNMP Threshold Interface Parameters A-8
DCM Global Parameters A-14
BOOTP and DHCP Parameters A-19
BOOTP Relay Agent Interface Parameters A-19
BOOTP Address Parameters A-21
BOOTP Client Interface Address Parameters A-23
BOOTP Preferred Server Configuration Parameters A-24
RARP Interface Parameters A-26
RARP Address Parameters A-26

Appendix B
Default Parameter Settings

SNMP Parameters B-1
DCM Global Parameters B-3
BOOTP and DHCP Parameters B-4
RARP Parameters B-5

Index

Figures

Figure 2-1. Role of SNMP 2-3
Figure 2-2. Sample RMON Configuration 2-11
Figure 2-3. Bay Networks RMON Architecture 2-12
Figure 2-4. BOOTP Client and Server on the Same Physical Network 2-25
Figure 2-5. BOOTP Client and Server on Different Physical Networks 2-26
Figure 2-6. BOOTREQUEST and BOOTREPLY Fields 2-27
Figure 2-7. Identifying DHCP Servers 2-31
Figure 2-8. Fields in a DHCP Packet 2-32
Figure 2-9. Requesting and Receiving IP Information 2-33
Figure 2-10. RARP Server Supplying an IP Address 2-35
Figure 5-1. Enabling BOOTP in a Sample Network 5-4

Tables

Table 2-1. Severity Levels 2-6
Table 2-2. Example of Threshold and Severity Settings 2-8
Table 2-3. DRAM and RMON Memory Size 2-18
Table 2-4. Maximum Number of Hosts 2-21
Table 2-5. Default Size for Capture Buffer 2-23
Table 3-1. Trap Types Transmitted by the SNMP Agent 3-6
Table 4-1. Optivity Analysis RMON-based Tools 4-8
Table B-1. SNMP Global Parameters B-1
Table B-2. SNMP Community Parameters B-1
Table B-3. SNMP Manager Parameters B-2
Table B-4. SNMP Trap Interface Parameters B-2
Table B-5. SNMP Threshold Global Parameters B-2
Table B-6. SNMP Threshold Interface Parameters B-2
Table B-7. DCM Global Parameters B-3
Table B-8. BOOTP Relay Agent Interface Parameters B-4
Table B-9. BOOTP Address Parameters B-4
Table B-10. BOOTP Client Interface Address Parameters B-4
Table B-11. BOOTP Preferred Server Configuration Parameters B-5
Table B-12. RARP Interface Parameters B-5
Table B-13. RARP Address Parameters B-5

About This Guide

If you are responsible for configuring and managing Bay Networks® routers or BayStream™ platforms, read this guide to learn how to configure and customize Simple Network Management Protocol (SNMP), remote monitoring (RMON), Bootstrap Protocol (BOOTP), Dynamic Host Configuration Protocol (DHCP), and Reverse Address Resolution Protocol (RARP).

Refer to this guide for

- Instructions for starting SNMP, RMON, BOOTP, DHCP, and RARP using default parameter values supplied by the software (Chapter 1)
- Conceptual information to help you decide how to configure SNMP, RMON, BOOTP, DHCP, and RARP on your network (Chapter 2)
- Instructions for customizing SNMP (Chapter 3)
- Instructions for configuring and managing the data collection module (DCM) for RMON (Chapter 4)
- Instructions for customizing BOOTP (Chapter 5)
- Instructions for customizing DHCP (Chapter 6)
- Instructions for customizing RARP (Chapter 7)
- Descriptions of SNMP, RMON, BOOTP, DHCP, and RARP parameters and instructions for editing them (Appendix A)
- Default parameter settings (Appendix B)

Before You Begin

Before using this guide, you must complete the following procedures:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers and BNX Platforms*, *Connecting BayStack AN and ANH Systems to a Network*, or *Connecting ASN Routers and BNX Platforms to a Network*).

Make sure that you are running the latest version of Bay Networks Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7-10xx to Version 11.0*.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`

separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu. Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

ASN.1	abstract syntax notation
BOOTP	Bootstrap Protocol
CMIP	Common Management Information Protocol
DCM	data collection module
DHCP	Dynamic Host Configuration Protocol
DLCI	Data Link Control Interface
FDDI	Fiber Distributed Data Interface
IP	Internet Protocol
MAC	media access control
PDU	Protocol Data Unit
PVC	permanent virtual circuit
RARP	Reverse Address Resolution Protocol
RIP	Routing Information Protocol
RMON	remote monitoring
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
WAN	wide area network

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from the Bay Networks Press™ at the following telephone or fax numbers:

- Telephone - U.S./Canada 1-888-4BAYPRESS
- Telephone - International 1-510-490-4752
- Fax 1-510-498-2609

You can also use these numbers to request a free catalog of Bay Networks Press product publications.

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Service FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus℠ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- with response times ranging to 4 hours, depending on local country conditions.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 916-8880 (direct)	(508) 670-8766
Europe	(33) 92-4-968-300	(33) 92-4-968-301
Asia/Pacific	(612) 9927-8800	(612) 9927-8811
Latin America	(561) 988-7661	(561) 988-7750

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *http://www.baynetworks.com*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *ftp://support.baynetworks.com* (134.177.3.26), this site combines and organizes support files and documentation for the entire Bay Networks product suite. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source[SM] CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh, Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been redesigned to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dialup number in the United States, call CompuServe at 1-800-524-3388. Outside the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you are online with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS℠ is the Bay Networks free 24-hour fax-on-demand service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside North America, toll calls can be made to 1-408-495-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-4-968-968	(33) 92-4-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Chapter 1
Starting SNMP, RMON, BOOTP, DHCP, and RARP Services

This chapter tells you how to start SNMP, BOOTP, DHCP, and RARP services and configure them on an IP interface using the default parameter values. It also describes how to start RMON (remote monitoring) for data collection by enabling the Ethernet data collection module (DCM) with a default configuration.

SNMP, BOOTP, DHCP, and RARP services all use the Internet Protocol (IP) for message transport. To use any of them on a router interface, you must enable IP services on that interface.

For detailed background information about these protocols and how they work, refer to Chapter 2. For information on how to customize these protocols by changing their default values, refer to Chapters 3 through 7. For information about changing the default settings, refer to Appendix A.

Before You Begin

Before you can start SNMP, RMON, BOOTP, DHCP, and RARP services on a router, you must

- Create and save a configuration file
- Retrieve the configuration file in local, remote, or dynamic mode
- Specify router hardware if this is a local-mode configuration

If you have any questions about how to perform any of these preliminary tasks, refer to *Configuring Routers*.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the management information base (MIB) object ID. This process is equivalent to modifying parameters using Site Manager.

For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: We strongly recommend that you use the Technician Interface for minor MIB adjustments only. The Technician Interface does not validate parameter entries. Entering an invalid value can corrupt your configuration.

Starting SNMP Services

Before you can use SNMP, you must enable IP services. When you enable IP services, you are required to configure only a few parameters; the system supplies default values for the remaining parameters.

You can accept the default values or edit IP global parameters to customize IP. For information about editing IP global parameters, refer to *Configuring IP Services*.

Enabling IP on an Interface

IP runs on all slots that contain IP interfaces. When you add an IP interface to a circuit, Site Manager enables IP on the slot. When you set IP global parameters, you are affecting the way IP operates on all slots where it is configured.

To enable IP services on an interface:

1. **In the Configuration Manager window, select the link- or net-module connector on which you are enabling IP services, or configure a WAN circuit if this connector requires one.**

   The Select Protocols window opens.

Note: The Select Protocols window displays only those protocols that the circuit type supports.

2. **Select IP from the Select Protocols window and click on OK.**

   The IP Configuration window opens.

3. **In the IP Configuration window, specify an IP address for this interface.**

   There is no default for the IP address. You must supply an address or enter 0.0.0.0 to indicate that this is an unnumbered interface. (For information about unnumbered interfaces, refer to *Configuring IP Services*.)

4. **Edit or accept default values for the remaining IP interface parameters.**

   - To accept the default values, click on OK
   - The Configuration Manager window opens. You can now customize IP interface parameters.
   - To edit IP interface parameters, click on Details.
   - Refer to *Configuring IP Services* for information about editing IP interface parameters.

Customizing IP

The instructions in this chapter show you how to start IP using the default values and settings. For information about modifying IP settings, refer to *Configuring IP Services*.

Starting RMON

Before you can use RMON, you must

1. Install an Ethernet DCM module in each router from which you want to collect RMON statistics. The Ethernet DCM physically connects to the BayStack™ AN® or BayStack ANH™ base module.

   Refer to *Installing an N11 Data Collection Module (DCM) in a BayStack AN* or *Installing an N11 Data Collection Module (DCM) in an 8-Port ANH* for detailed instructions on physically installing the Ethernet DCM hardware in a BayStack AN or BayStack ANH router.

2. Install the latest Ethernet DCM software image in the Ethernet DCM's Flash memory to ensure that the Ethernet DCM runs properly on your router.

To run RMON on a Version 11.0 or later Bay Networks router, the router must be running a Version 1.4 or later DCM image. If the router has an earlier version of DCM, the RMON Summary application returns an error message telling you that the router does not support RMON. For information about upgrading your router and the DCM image, refer to *Upgrading Routers from Version 7-10.xx to Version 11.0*. The upgrade guide also describes how to determine the version of DCM you are currently running.

3. Configure an Ethernet interface for each LAN segment you want to monitor.
4. Install and configure on your network management station an RMON network management application, such as Optivity® LAN or Optivity Analysis, to view and analyze statistics generated by the Ethernet DCM.

Enabling the Ethernet DCM

The quickest way to begin using RMON is to enable a newly installed data collection module (DCM). The DCM runs the RMON agent software that gathers statistics for Ethernet remote monitoring support. You enable the Ethernet DCM by creating the data collection module middleware (DCMMW) software configuration using the default configuration parameter values. For information about modifying the default configuration parameters, refer to Chapter 4.

To enable the Ethernet DCM from the Configuration Manager window:

1. **Select Platform > DCM 11.0 and later > Create Base Module DCM.**

   The Edit Base Module DCM Parameters window opens.

2. **Click on OK to accept the default configuration parameters.**

Once the Ethernet DCM is enabled and collecting statistics, you can use Optivity LAN software or a third-party RMON network management application to view and analyze statistics.

Customizing the Ethernet DCM

For information about customizing the DCMMW configuration parameters, refer to “Managing the Ethernet DCM” in Chapter 4.

Starting BOOTP Services

Before you can run BOOTP services, you must enable IP on the router. You can, however, enable IP and BOOTP on the router simultaneously. If you want to add BOOTP to a circuit on which you have already configured IP, refer to *Configuring Routers* for more information about adding a protocol.

When you enable BOOTP, you are required to configure only a few parameters. The Configuration Manager supplies values for the remaining parameters.

Enabling BOOTP on an Interface

When you select either a link- or net-module connector, or when you finish configuring a WAN circuit, the Select Protocols window opens.

Note: The Select Protocols window displays only those protocols that the circuit type supports.

To enable BOOTP on an interface:

1. **Select BOOTP from the Select Protocols menu.**

   When you select BOOTP, you automatically select IP.

2. **Click on OK.**

   The IP Configuration window opens.

3. **Edit the IP configuration parameters as described in "Enabling IP on an Interface," earlier in this chapter.**

4. **Click on OK.**

Customizing BOOTP

For information about customizing BOOTP parameters, refer to Chapter 5.

Starting DHCP

Before you can enable DHCP services, you must enable IP and BOOTP on the router. You can, however, enable IP, BOOTP, and DHCP on the router simultaneously. If you want to add BOOTP and DHCP to a circuit on which you have already configured IP, refer to *Configuring Routers* for information about adding a protocol.

When you enable BOOTP and DHCP, you are required to configure only a few parameters. The Configuration Manager supplies default values for the remaining parameters.

Enabling DHCP on an Interface

When you select either a link- or net-module connector, or when you finish configuring a WAN circuit, the Select Protocols window opens.

Note: The Select Protocols window displays only those protocols that the circuit type supports.

To enable DHCP on an interface:

1. **Enable BOOTP on the interface.**

   Refer to "Enabling BOOTP on an Interface," earlier in this chapter, for instructions.

2. **Access the BOOTP Relay Agent Interface Table window.**

   Refer to "Customizing BOOTP Relay Agent Parameters" in Chapter 5 for instructions.

3. **Set the Pass Through Mode parameter to DHCP or to BOOTP and DHCP.**

   This action allows you to select either DHCP or BOOTP and DHCP for the Pass Through Mode parameter in other windows.

Site Manager: Pass Through Mode parameter: page A-20

4. **Click on Apply.**

5. **Edit the other parameters in this window.**

   Refer to the section “Customizing BOOTP Relay Agent Parameters” in Chapter 5 for guidelines.

Customizing DHCP

For information about modifying DHCP parameters, refer to Chapter 6.

Starting RARP Services

Before you can enable RARP services, you must enable IP on the router. You can, however, enable IP and RARP services on the router simultaneously. If you want to add RARP to a circuit on which you have already configured IP, refer to *Configuring Routers* for information about adding a protocol.

When you enable RARP services, you are required to configure only a few parameters. The Configuration Manager supplies default values for the remaining parameters.

Enabling RARP on an Interface

When you select either a link- or net-module connector, or when you finish configuring a WAN circuit, the Select Protocols window opens.

Note: The Select Protocols window displays only those protocols that the circuit type supports.

To enable RARP on an interface:

1. **From the Select Protocols menu, select Reverse ARP.**

   When you select RARP, you automatically select IP.

2. **Click on OK.**

   The IP Configuration window opens.

3. **Edit the IP configuration parameters as described in "Enabling IP on an Interface," earlier in this chapter.**

4. **Click on OK.**

Customizing RARP

For information about modifying RARP parameters, refer to Chapter 7.

Chapter 2
SNMP, RMON, BOOTP, DHCP, and RARP Concepts

This chapter describes the concepts behind SNMP, RMON, BOOTP, DHCP, and RARP services and how we implement them in Bay Networks routers. You can use this information to decide how to customize SNMP, RMON, BOOTP, DHCP, and RARP parameters for your system.

SNMP Overview

SNMP is a simple request/response protocol that communicates management information between two types of SNMP software entities: SNMP *applications* (also called SNMP *managers*) and SNMP *agents*.

SNMP applications contain manager software that runs on a network management station (also known as an SNMP client), such as a PC or a workstation. The manager software implements the protocols used to exchange data with SNMP agents. SNMP applications issue queries to gather information about the status, configuration, and performance of external network devices, called *network elements* in SNMP terminology. Network elements contain an agent and perform the network management function that the network management stations request.

The Bay Networks Site Manager software is an example of a network management station, and the Bay Networks Backbone Node (BN) router is an example of a network element.

The *SNMP agent* is a software entity that responds to information and action request messages (SNMP Set and Get requests) sent by a network management station (your Site Manager workstation). The messages exchanged between manager and router SNMP agents in turn enable you to access and manage objects in an active or inactive (stored) MIB on a particular router.

The agents also send unsolicited reports (called *traps*) back to the network management station when certain network activity occurs. An example of a trap is an overload condition as defined by the packet load's crossing some threshold. You use the management station to configure, monitor, and receive trap messages from other network devices configured as SNMP agents. The management station can get and set objects in the agents and can receive traps from the agents. The management station, therefore, has the capability to "manage" a number of agents.

SNMP Messages

SNMP managers and network elements communicate with each other by sending SNMP messages (Figure 2-1). The management station issues three types of SNMP messages to retrieve single or multiple object variables:

- *GetRequest* message
- *GetNextRequest* message
- *SetRequest* message

The agent acknowledges all three types of messages in the form of a *Get Response* message, which is passed to the management application. In addition, an agent may issue a trap to the network management station to identify the occurrence of a condition, such as a threshold that exceeds a predefined value.

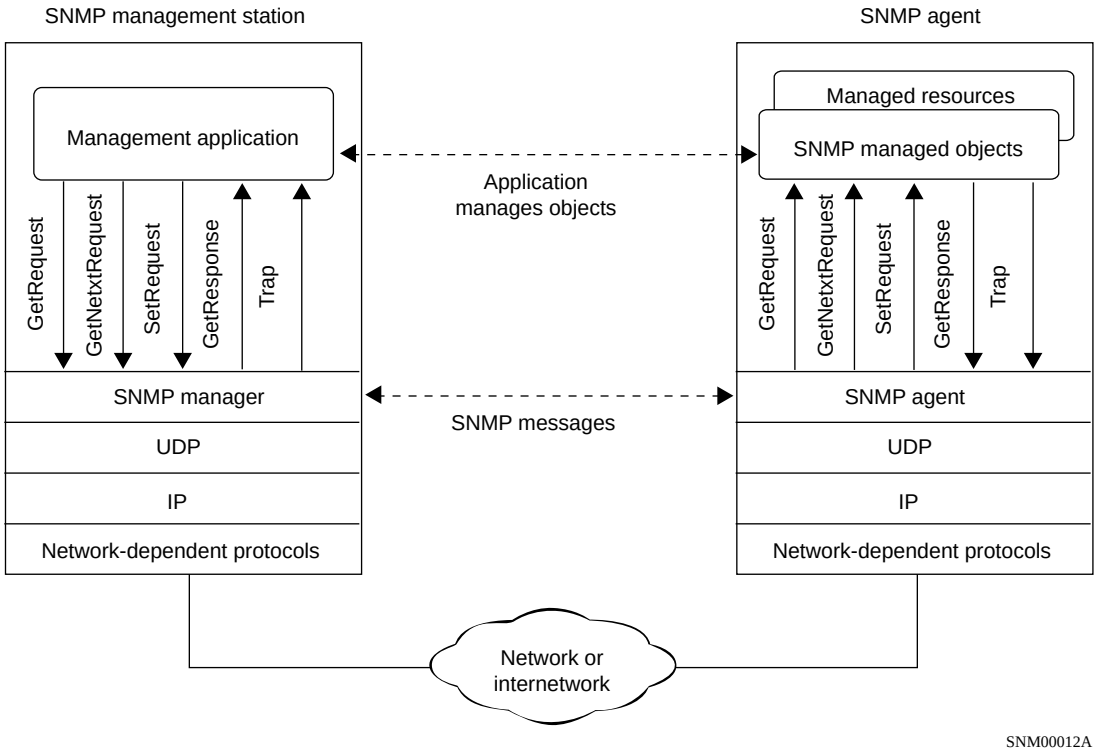

Figure 2-1. Role of SNMP

SNMP Communities

For security reasons, the SNMP agent validates each request from an SNMP manager before responding to the request, by verifying that the manager belongs to a valid SNMP *community.*

An SNMP community is a logical relationship between an SNMP agent and one or more SNMP managers. You define communities locally at the agent. The agent establishes one community for each desired combination of authentication and access control characteristics. You assign each community a unique name (within the agent), and all members of a community have the same access privileges, either read-only or read-write:

- Read-only: members can view configuration and performance information
- Read-write: members can view configuration and performance information, and also change the configuration

By defining a community, an agent limits access to its MIB to a selected set of management stations. By using more than one community, the agent can provide different levels of MIB access to different management stations.

All SNMP message exchanges consist of a community name and a data field, which contains the SNMP operation and its associated operands. You can configure the SNMP agent to receive requests and send responses only from managers that are members of a known community.

If the agent knows the community name in the SNMP message and knows that the manager generating the request is a member of that community, it considers the message to be authentic and gives it the access allowed for members of that community. Thus, the SNMP community prevents unauthorized managers from viewing or changing the configuration of a router.

SNMP Implementation Notes

This section contains information about features specific to the Bay Networks implementation of SNMP.

Internet Protocol (IP)

SNMP uses the User Datagram Protocol (UDP) to transport its messages. You must enable IP to use UDP and SNMP.

Events and Traps

An *event* is a change in the operating status of a router. The router stores the event as a single entry in a memory-resident log.

An *event log message* provides a brief description of an event, along with the event code associated with that event.

A *trap* is an event that the router transmits to the network management station.

SNMP allows you to configure which event log messages the agent sends to the network management station as traps. You select these traps based on slot, protocol entity, and severity level. You can also specify up to 50 *exceptions*, which are traps that the agent always sends, or never sends, regardless of slot and regardless of how you configure the trap parameters. Refer to "Configuring Traps on the Router" in Chapter 3 for information about how to specify which traps the agent sends.

Protocol Entities

Events are always associated with a particular protocol entity. An entity is the software that generates a message. Entities include Bay Networks software dedicated to the operation of a software service, such as TFTP and IP, and the GAME operating system.

Both events and entities are assigned entity codes. Together, this pair uniquely identifies a Bay Networks router or BNX platform event. Refer to *Event Messages for Routers and BNX Platforms* for a complete list of entities (both their abbreviations and full names) and associated entity codes.

Severity Levels

Event and trap messages are always associated with one of five severity levels. Table 2-1 describes the severity levels and lists the code that corresponds to each one. This guide does not cover Debug messages, because these are for Bay Networks internal use only.

Table 2-1. Severity Levels

Severity	Description	Code
Information	Indicates routine events that usually require no action.	2
Warning	Indicates that a service acted in an unexpected manner.	4
Fault	Indicates a major service disruption, usually caused by a configuration, network, or hardware problem. The entities involved keep restarting until the problem is resolved.	8
Trace	Indicates information about each packet that traversed the network. Bay Networks recommends viewing this type of trap message only when diagnosing network problems.	10
Debug	Indicates information that Bay Networks Customer Support uses. These messages are not documented.	1

Refer to *Event Messages for Routers and BNX Platforms* for detailed information about entities and severity levels.

SNMP Trap Format

Some third party network management applications, such as NetExpert, OpenView, and SunNet, allow you to trigger a desired operation when a specific SNMP trap is received. This section describes the SNMP trap format.

The router or BNX platform transmits Bay Networks event log traps as a 32-bit value as follows:

- Octets 1 and 2 (the most significant 16 bits) of the specific trap ID contain values of 1 and 0 respectively to identify a Bay Networks event log trap.
- Octet 3 of the specific trap ID contains a code that identifies the software entity that generated the trap.
- Octet 4 of the specific ID contains the event code that, in conjunction with the entity code, uniquely identifies the event.

Each 32-bit value is accompanied by three variable bindings that convey the event string that describes the trap condition, the slot that hosts the entity that generated the trap, and the trap severity (refer to Table 2-1).

Refer to *Event Messages for Routers and BNX Platforms* for detailed information about the SNMP trap format.

Thresholds

SNMP uses a management information base (MIB) to manage the router. The MIB includes an extensive collection of statistics (MIB *variables*) that track the router's performance and provide early warnings of abnormal operating conditions.

With the Site Manager threshold feature, you can configure the agent to automatically notify you when specific statistics (or *instances* of the variable) reach certain levels.

You can set a threshold for any integer, counter, gauge, or time-tick variable in the MIB. Using the threshold parameters you

- Select the polling interval, which specifies how often the agent checks the statistic to see if its value has reached the threshold
- Set three threshold values (high, medium, and low)
- Specify the threshold action as *Lessthan* or *Greaterthan*

For information about setting thresholds, refer to "Configuring Thresholds" in Chapter 3.

When the statistic reaches the threshold, the agent generates an event. You specify the severity level at which you want the manager to log the event. Table 2-1 lists the available severity levels and their suggested meanings. Depending on how you configure the SNMP trap parameters (refer to "Configuring Traps on the Router" in Chapter 3), the agent may also send the threshold exception as an SNMP trap.

The Site Manager threshold feature is functionally similar to the RMON Alarm and Event facility, except for some minor differences. The Site Manager threshold feature provides three-tiered thresholds and defines a user-definable hysteresis mechanism. The RMON Alarm and Event facility provides a two-tiered proprietary thresholds system.

Threshold Example

Suppose you want SNMP to warn you if the number of high-priority (Priority Level 1) packets queued for transmission is approaching the maximum number supported by an interface. This maximum value is specified by the wfCctOptsCngcCfgQp1Threshold MIB object. Using the threshold parameters, you set a threshold for wfCctOptsCngcCfgQp1Threshold equal to 205.

You also set the polling interval to 20 seconds to indicate that, every 20 seconds, the agent should check variables for which you have configured thresholds. You set the threshold action to *Greaterthan* and set the threshold levels and severity of events to the values listed in Table 2-2.

Table 2-2. Example of Threshold and Severity Settings

Threshold Level	Low	Medium	High
Depth of Priority 1 transmit queue	102 (40% of capacity)	153 (60% of capacity)	205 (80% of capacity)
Severity of event	INFO	INFO	WARNING

When you add this threshold to the MIB, the agent polls the variable wfCctOptsCngcCfgQp1Threshold every 20 seconds and responds as follows:

- If its value is greater than 102, but less than or equal to 153, the manager logs an informational event indicating that the queue depth exceeded the low threshold.
- If its value is greater than 153 but less than or equal to 205, the manager logs an informational event indicating that the queue depth exceeded the medium threshold.
- If its value is greater than 205, the manager logs a warning event indicating that the queue depth exceeded the high threshold.

Event Message Format

By default, the threshold event messages include the MIB object identifier (OID) of the variable that exceeded the threshold, the value of the variable, and the threshold level exceeded.

For example, if the wfCctOptsCngcCfgQp1Threshold variable has a value of 120, the agent generates an event message similar to the following:

```
#1:08/27/96 10:53:20.802 INFO SLOT 2 STA CODE: 6
Object 1.3.6.1.4.1.18.3.5.1.4.10.1.24 with value = 120 units/ hour is
> low threshold.
```

You can, however, identify objects more easily by configuring the software to report the object name rather than the OID in the event message. To configure the software to report the object name in the event message, use the Threshold Label parameter (refer to Appendix A).

For example, if you set the Threshold Label parameter to **wfCctOptsCngcCfgQp1Threshold**, the agent generates an event message similar to the following:

```
#1:08/27/96 10:53:20.802 INFO SLOT 2 STA CODE: 6
Object wfCctOptsCngcCfgQp1Threshold with value = 120 units/ hour is
> low threshold.
```

State of a Threshold

If the collision rate stays above a threshold for an extended period of time, the agent continues to generate a new event every 5 seconds. You can specify the maximum number of event messages you want the agent to generate before it changes the threshold's state to *held*.

When the threshold is in a held state, the agent does not generate new events unless the statistic exceeds the threshold at a different level. If the statistic does not exceed any threshold for a specified number of polling periods, the agent no longer considers the threshold held.

Memory Considerations

Polling statistics to determine whether they have reached a threshold and reporting events when variables exceed thresholds require router processing capacity. When you set many thresholds and use shorter polling intervals, the router performance will probably decline.

RMON Overview

RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing you to capture realtime information across the entire network. The RMON standard is an SNMP MIB definition described in RFC 1757 (formerly 1271) for Ethernet.

The RMON MIB provides a standard method to monitor the basic operations of the Ethernet, providing inoperability between SNMP management stations and monitoring agents. RMON also provides a powerful alarm and event mechanism for setting thresholds and for notifying you of changes in network behavior.

You can use RMON to analyze and monitor network traffic data within remote LAN segments from a central location. This allows you to detect, isolate, diagnose, and report potential and actual network problems before they escalate to crisis situations. For example, the Ethernet DCM can identify the hosts on a network that generate the most traffic or errors.

RMON allows you to set up automatic histories, which the RMON agent collects over a period of time, providing trending data on such basic statistics as utilization, collisions, and so forth. Using a network management application such as Optivity LAN or Optivity Analysis, you can retrieve histories to understand network usage patterns. Because RMON automates this data collection and provides better data to the planning process, the process is easier and the outcome more accurate.

How RMON Works

A typical RMON configuration consists of a central *network management station* and a remote monitoring device, called an RMON *agent*. The network management station can be a Windows-based or UNIX-based workstation or PC running a network management application, such as Optivity Analysis. From the management station, you can issue SNMP commands requesting information from the RMON agent. The RMON agent sends the requested information to the management station, which then processes and displays this information on its console.

The RMON agent is software that resides on a DCM within a Bay Networks BayStack AN or ANH router on a remote network. As packets travel across the network, the RMON agent continuously collects and analyzes Ethernet data in real time on a remote LAN segment and stores the data locally in the Ethernet DCM according to the RMON MIB specification, defined in RFC 1757.

You can have multiple RMON agents running in different segments of the network, usually one per subnet (Figure 2-2).

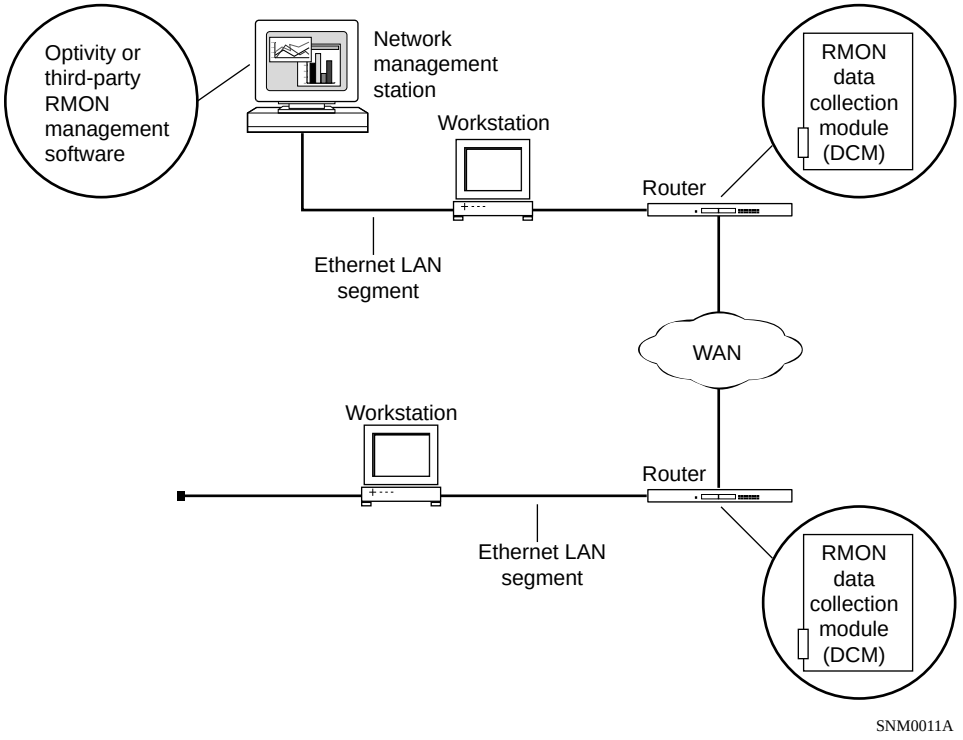

Figure 2-2. Sample RMON Configuration

RMON Architecture

The Bay Networks implementation of RMON consists of the BayStack AN or BayStack ANH base module, a data collection module (DCM), data collection module middleware (DCMMW), and the DCM Flash memory module (Figure 2-3).

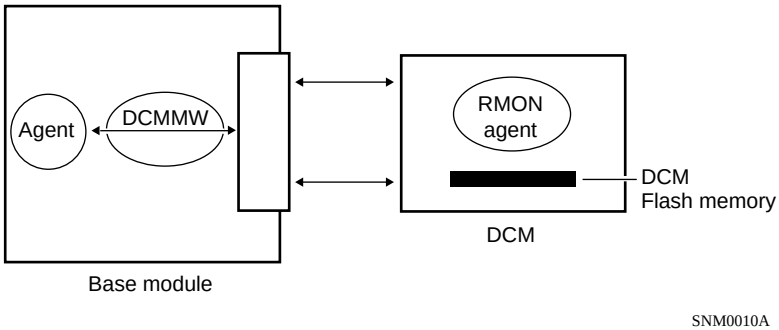

Figure 2-3. Bay Networks RMON Architecture

The Ethernet DCM physically connects to the BayStack AN or BayStack ANH base module. The Ethernet DCM contains a Flash memory module for its own boot image and configuration file. The Ethernet DCM runs the RMON agent software that

- Gathers statistics by monitoring packets on an Ethernet segment
- Stores the information according to the RMON MIB specification, in compliance with RFC 1757

To communicate with the RMON agent software on the Ethernet DCM, the BayStack AN or BayStack ANH uses a software subsystem, called the DCMMW. This software subsystem enables and configures an installed Ethernet DCM, and allows you to modify the Ethernet DCM configuration, boot the Ethernet DCM, and disable the Ethernet DCM using Site Manager. You can use an SNMP-based network management application that supports RMON to view RMON statistics.

RMON MIB Groups

The Ethernet DCM board supports a set of RMON MIB groups. RFC 1757 defines the function and organization of these groups. Bay Networks implements the following groups in its RMON agent for the BayStack AN and BayStack ANH routers:

- Statistics
- History
- Host
- HostTopN
- Matrix
- Filter
- Capture

The router base module supports the following groups:

- Alarm
- Event

Several of the RMON groups in the MIB contain control and data tables. Control tables contain control parameters that specify which statistics you want to access and collect. You can view and change many entries in a control table. Data tables contain statistics the agent collects; usually you can only view entries in these tables.

The following sections describe the function of each group and the tables that each group defines. Refer to RFC 1757 for the following information:

- A list of all the parameters that appear in a control table
- The read/write status of a control parameter
- The default values for control parameters with read/write status
- A list of all the objects that appear in a data table

Statistics Group

The Statistics group records data that the Ethernet DCM measures on network interfaces. The Ethernet DCM creates one entry for each Ethernet interface it monitors and places the entry in the EtherStatsTable. The EtherStatsTable also contains control parameters for this group.

History Group

The History group contains a control and data collection function. The control function manages the periodic statistical sampling of data from networks and specifies control parameters, such as the frequency of data sampling, in the historyControlTable.

The history function records periodic statistical samples from Ethernet networks, for example, interval start time and number of packets. This function places the statistical samples in the etherHistoryTable.

Host Group

The Host group identifies hosts on the network by recording the source and destination MAC addresses in good packets, and places the information in the hostTable. This group also records the time it discovered a host on the network in the hostTimeTable. The hostControlTable specifies control parameters such as which monitoring operations the Ethernet DCM performs, and contains some information about the monitoring process.

HostTopN Group

The HostTopN group ranks hosts according to a statistic type. For example, you might want to rank the hosts by the number of errors they generate. Control parameters for this group appear in the hostTopNControlTable, and data this group generates appears in the hostTopNTable. To use the HostTopN group, you must set up the Host group.

Matrix Group

The Matrix group stores statistics for an interchange between hosts at different addresses. This group's control parameters, such as number of hosts, appear in the matrixControlTable. When the Matrix group receives information from a good packet, it places data in both the matrixSDTable and the matrixDSTable.

Filter Group

The Filter group specifies what type of packets the Ethernet DCM should capture. Filter control parameters, such as the minimum length of the packets to capture, appear in the filterTable. Associated with each filter is a *channel* (a specific path along which data flows). Control parameters in the channelTable define how and where the filtered packets flow.

Capture Group

The Capture group enables the capture of packets that satisfy the Filter group control parameters for a particular channel. Control parameters in the bufferControlTable specify how to transfer data from the channelTable to the captureBufferTable. For example, you can specify the maximum number of octets from each packet that the group should store in the captureBufferTable. To use the Capture group, you must set up the Filter group.

Alarm Group

The Alarm group allows you to set an alarm threshold and a sampling interval to enable the RMON agent to generate alarms on any network segment it monitors. Alarm thresholds can be based on absolute or delta values so that you can be notified of rapid spikes or drops in a monitored value.

Each alarm is linked to an event in the event group. An event defines an action that will be triggered when the alarm threshold is exceeded.

The alarm group periodically takes statistical samples from variables in the Ethernet DCM and compares them to previously configured thresholds. The Alarm Table stores configuration entries that define a variable, a polling period, and threshold parameters. If the RMON agents determines that a sample crosses the threshold values, it generates an event. The RMON agent monitors any variables that resolve to an ASN.1 primitive type of integer (integer, counter, gauge, or TimeTick) in this way.

You can specify rising or falling thresholds, indicating network faults such as slow throughput or other network-related performance problems. You specify rising thresholds when you want to be notified that an alarm has risen above the threshold you specified. You specify falling thresholds when you want to be notified that the network is behaving normally again. For example, you might specify a falling threshold of 30 collisions per second to indicate a return to acceptable behavior.

When you configure an alarm condition, you must define the following values:

- The monitoring interval over which data is sampled
- The variable to be sampled
- Rising and falling thresholds used to detect when network trouble starts and when it ends

- The event that takes place when a rising threshold is crossed
- The event that takes place when a falling threshold is crossed

You can specify thresholds for numeric variables, such as integer, counter, gauge, or TimeTick.

Event Group

The Event group allows for the generation of an SNMP trap, the generation of a log entry, or both, for any event you choose. An event can occur when the sample variable exceeds the alarm threshold or a channel match event generated on an Ethernet DCM. Traps can be delivered by the RMON agent to multiple management stations. For information on setting trap destinations, refer to Chapter 3.

You can set up events to either record the monitoring information or to notify the network management station. The Event group includes an Event Table and a Log Table. The Event Table defines the notification that takes place when an event is triggered. One form of notification is to write an entry in the Log Table.

Each entry in the Event Table identifies an event that can be triggered and indicates an action, such as writing a log entry to the Log Table or sending an SNMP trap to the network management station. The event can trigger any of the following actions:

- The system sends an SNMP trap to the network management station.
- The management station is notified immediately. The management station determines how to react to the SNMP trap.
- The system logs the event in the Log Table in the agent system.
- The management station can retrieve the information stored in the Log Table for further analysis. For example, the information collected can be used to select proper threshold values.
- The system sends an SNMP trap and logs the event in the Log Table.

The Log Table is a read-only data table for the network management station. It records each event that needs to be logged. It provides the event number, an index that distinguishes occurrences of the same event, the time at which the event occurred, and the event description. You are not required to configure the Log Table.

Event Trap Considerations

In order for RMON to generate trap events, you must set up the SNMP managers table based on the SNMP community names (for example, Public) you are using with the network management application (for example, Optivity LAN or Optivity Analysis) and the hosts on which you are running applications. If you fail to make these changes, the router will be unable to send trap events to the network management station. Refer to Chapter 3 for instructions on how to set up an SNMP managers table.

When you set up the SNMP managers table, you can use the SNMP community names that the network management application uses and modify the trap receiving tables on the router to use these names. Or, you can configure the router to use specific SNMP community names and modify the network management software to use these names.

When configuring SNMP community managers, you must assign each manager a specific IP address; you cannot specify a wildcard for the community manager address. Also, you must configure community managers to receive all traps, not just generic traps. You do this by changing the Trap Types parameter in the SNMP Manager window from “Generic” (the default) to “All.” For more information about changing communities and community manager parameters, refer to Chapter 3.

RMON Interoperability Issues

This section describes RMON memory use and interoperability issues you should consider when using RMON network management applications with the Ethernet DCM.

This section assumes that you have a good understanding of each RMON group, and does not refer to the low-level details of the MIB, such as RMON MIB objects. Refer to “RMON MIB Groups,” earlier in this chapter, and RFC 1757 for information about each RMON group.

RMON Applications

Some network management applications automatically set up their own configurations for an RMON group, without checking to see if the RMON agent already has a default configuration. In addition, when you terminate those applications, they may not remove the configurations they set up for the RMON agent. These features can result in the RMON agent using excessive amounts of memory and processing power.

Example

When you enable an Ethernet DCM, the RMON agent automatically creates a History configuration. Suppose you then start a third-party RMON History application that creates its own History configuration for the agent. The RMON agent stores the data in two places, wasting memory.

In addition, when you terminate the third-party RMON application, it does not remove its History configuration, using memory and processing power indefinitely.

You can release these resources only by using another application, such as the SNMP tool or network management station, or by resetting the Ethernet DCM. If you use too many resources for an RMON task, the DCM can run out of memory for other RMON tasks and perform more slowly.

RMON Memory Use

The total amount of available RMON memory depends on the dynamic random access memory (DRAM) in the Ethernet DCM (Table 2-3).

Table 2-3. DRAM and RMON Memory Size

Installed DRAM (MB)	Available RMON Memory in Bytes
2	162,578
4	2,077,330
8	5,222,034
16	12,561,042

If the RMON memory pool is full or if the RMON agent reaches an implementation limit, the agent responds to an SNMP **set** command on an RMON control table entry with an SNMP GEN-ERROR.

The following sections describe how much memory you need to

- Configure an RMON group (for example, to configure the Matrix group or to configure the Filter and Capture groups)
- Store the data for an RMON group (for example, to store the packets on Ethernet DCM captures)

In the following sections, the word *configuration* means the set of control tables for a group. For example, a Matrix configuration includes only the matrixControlTable. Note that you can create more than one configuration for some RMON groups. For example, you can create more than one History configuration, allowing you to specify different intervals for sampling statistics.

Interoperability Issues and Memory Use for RMON Groups

You should understand the following issues about each RMON group's memory requirements and ability to operate with third-party RMON network management applications.

Statistics Group

When you enable the Ethernet DCM, the RMON agent automatically creates a Statistics configuration that records data for each network interface. Through your RMON network management application, you can create as many Statistics configurations as memory permits, up to the RMON limit of 65,535 configurations.

If you create multiple configurations, it is possible to collect the same set of statistics for the same interface in multiple data tables. The absolute values of those statistics may vary from table to table, since the baseline of each statistics counter occurs when you create a configuration. You may prefer, however, to use only one Statistics configuration, to conserve memory for other RMON groups.

You need 200 bytes of memory for each Statistics configuration.

History Group

When you enable the Ethernet DCM, the RMON agent automatically creates a History configuration that collects History data at two intervals. The first configuration provides short-term history by sampling statistics every 30 seconds and holding up to 50 samples (in RMON terms, “buckets”). The second configuration provides long-term history by sampling statistics every 30 minutes and holding up to 50 buckets.

Through your RMON network management application, you can create as many History configurations as memory permits, up to the RMON limit of 65,535 configurations.You can also set the number of buckets a particular History configuration uses to as many as available memory allows. If you request more buckets than memory allows, the agent allocates enough buckets to fill available memory.

You need 504 bytes of memory for each History configuration (252 bytes each for the short-term and long-term History configurations).

The History data requires 52 bytes of memory per bucket. You calculate the total memory (in bytes) you need to store the data as follows:

number of buckets * 52 * 2 History configurations

This calculation shows that you need approximately 5.1 KB for the default setting of 50 buckets.

Host Group

When you enable the Ethernet DCM, the default setting (Disabled) for the RMON Default Host parameter will not create a Host configuration. To create a Host configuration, set the RMON Default Host parameter to Enable before you enable the Ethernet DCM. For instructions on how to enable the Ethernet DCM, refer to Chapter 1.

Some RMON network management applications expect the Ethernet DCM to set up a Host configuration, while others set up their own configurations.

Note: The RMON agent allows you to create only one Host configuration. Be sure to set the RMON Default Host parameter according to the expectations of the RMON network management application.

The Host configuration requires 148 bytes. The Host data requires 105 bytes of memory per host address the Ethernet DCM detects on a segment.

You specify the maximum number of host addresses that appear in the Host configuration by setting the RMON Max Host parameter when you enable an Ethernet DCM. If there is not enough memory for the number of hosts you request, the RMON agent sets the RMON Max Host parameter to the highest possible value. The number of addresses can range from 100 to 8,128 hosts, depending on the Ethernet DCM memory configuration. Table 2-4 shows recommended values for this parameter.

Table 2-4. Maximum Number of Hosts

Installed DRAM (MB)	Maximum Number of Hosts
2–4	2,048
5–8	4,096
9–16	8,128

You calculate the total memory (in bytes) you need for the host data as follows:

105 * value of the RMON Max Host parameter

HostTopN Group

To save memory and increase performance, there is no default configuration for the HostTopN group. You must create HostTopN configurations through your RMON network management application. You can create as many HostTopN configurations as memory permits, up to the RMON limit of 65,535 configurations.

Note: Before you create a HostTopN configuration, you must create a Host configuration.

Each HostTopN configuration requires 164 bytes. The HostTopN data requires 10 bytes of memory per host address the Ethernet DCM detects on a segment.

You calculate the total memory (in bytes) you need for the HostTopN data as follows:

10 * value of the RMON Max Host parameter

Refer to the previous section for information about setting the RMON Max Host parameter.

Matrix Group

When you enable the Ethernet DCM, the default setting (Disabled) will not set up the RMON Default Matrix parameter on the Ethernet DCM. To create a Matrix configuration, set the RMON Default Matrix parameter to Enable before you enable the Ethernet DCM (refer to *Connecting AN and ANH Systems to a Network* for details).

Some RMON network management applications expect the DCM to set up a Matrix configuration, while others set up their own configurations.

Note: The RMON agent allows you to create only one Matrix configuration. Be sure to set the RMON Default Matrix parameter according to the expectations of the RMON network management application.

The Matrix configuration requires 212 bytes. The Matrix data requires approximately 178 bytes of memory per source/destination pair the Ethernet DCM detects on a segment.

Filter and Capture Groups

Caution: The memory you need for a Filter/Capture configuration and for storing captured packets can easily exhaust all the available memory on an Ethernet DCM, particularly if the filters are not selective.

You must create Filter and Capture configurations through your RMON network management application. You can create as many filters and capture buffers as memory permits, up to the RMON limit of 65,535 configurations.

Memory requirements vary greatly according to the size and number of the filters and the size of the capture buffer. In most cases, you need 3 to 5 KB of memory for the Filter and Capture configuration.

The size of the capture buffer determines the amount of memory you need for the data. You can request the largest buffer size available by specifying a buffer size of -1 through your RMON network management application. When you specify -1 for the capture buffer size, the agent attempts to allocate a default buffer, depending on the DRAM in the Ethernet DCM (Table 2-5).

Table 2-5. Default Size for Capture Buffer

Installed DRAM (MB)	Default Size (KB)
2	32
4	64
8	256
16	512

You can also request a larger buffer size up to 15 MB. In any case, if there is not enough memory currently available to satisfy the request, the agent will provide a buffer that uses all available memory.

You can determine the maximum number of packets that an agent can capture in a buffer as follows:

buffer size/(packet slice size + 20 bytes)

Example

You specify a buffer size of 32 KB and a packet slice size of 1 KB. After checking the available memory, the RMON agent allocates the buffer size you requested. The buffer can hold a maximum of 32,768 / (1024 + 20), or 31 packets.

Note: The RMON agent allocates the full amount of memory you specify for the packet slice size to each packet, even if the packet size is smaller than this amount. For this reason, Bay Networks recommends that you set the packet slice size to the smallest size possible. The maximum packet size is 2 KB.

Alarm and Event Groups

When you enable the Ethernet DCM, the router does not create default Alarm or Event entries. We recommend that you create Alarm and Event entries using a network management application.

You can create as many Alarm or Event entries as memory permits, up to the RMON limit of 65,535 entries. The memory limitation for Alarm and Event groups is based on the memory resources allocated on the router base module rather than the Ethernet DCM memory resources. The RMON Alarm and Event groups are maintained by the router base module. All other RMON groups are supported on the Ethernet DCM.

Each Alarm entry requires 232 bytes. Each Event entry requires 542 bytes.

The Log Table can accommodate up to 65,535 entries. Each entry in the Log Table requires 267 bytes. You cannot delete log entry rows. Therefore, as events are triggered and the event type specifies logging, the Log Table increases in size. Although there is no way to delete a specific log entry, all log entries in the Log Table corresponding to a single event entry are deleted when the event entry is deleted.

BOOTP Relay Agent Overview

BOOTP is built on the client-server model and allows a diskless client to boot remotely from a server on the same network or on a different physical network. The client broadcasts a request to boot from a remote server. When a suitable server receives the BOOTREQUEST packet, it responds to the client by issuing a BOOTREPLY packet, which includes the client's IP address, the address of the gateway, and the address of a server. The server then transmits the boot file to the client via a transfer protocol, such as Trivial File Transfer Protocol (TFTP).

Figure 2-4 illustrates how BOOTP works when the client and the server are on the same network. The client transmits a BOOTREQUEST packet to the IP broadcast address (255.255.255.255). The server sends a BOOTREPLY packet to the client. Depending on the server's implementation, the server addresses the packet to either the broadcast or the client's IP address.

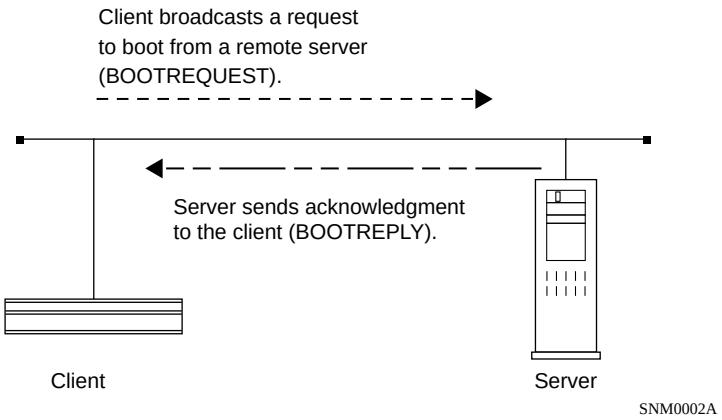

Figure 2-4. BOOTP Client and Server on the Same Physical Network

If, however, the client and the server are on different physical networks, a BOOTP *relay agent* (also known as a BOOTP gateway) must forward BOOTP packets to their correct destinations. When you configure a Bay Networks router for BOOTP services, the router acts as a BOOTP relay agent. Figure 2-5 illustrates how BOOTP works when the client and the server are on different physical networks.

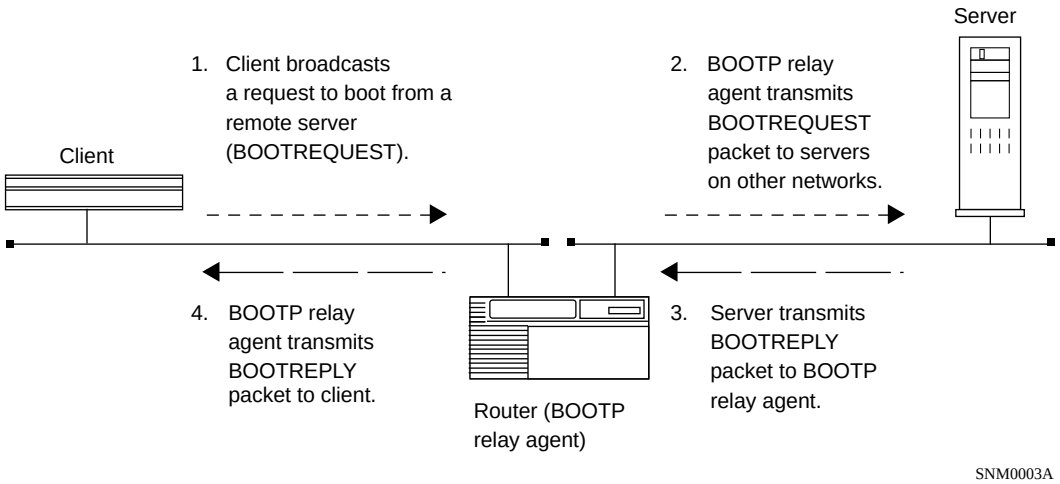
Server
1. Client broadcasts a request to boot from a remote server (BOOTREQUEST).
2. BOOTP relay agent transmits BOOTREQUEST packet to servers on other networks.
Client
4. BOOTP relay agent transmits BOOTREPLY packet to client.
3. Server transmits BOOTREPLY packet to BOOTP relay agent.
Router (BOOTP relay agent)
SNM0003A

Figure 2-5. BOOTP Client and Server on Different Physical Networks

The client transmits a BOOTREQUEST packet to the IP broadcast address (255.255.255.255). The router receives the BOOTREQUEST packet at an interface that you configured to receive BOOTREQUEST packets (an input interface). If the BOOTREQUEST packet has an address other than 255.255.255.255, the router drops the packet.

Figure 2-6 shows the fields in the BOOTREQUEST and BOOTREPLY packets.

Operation (1) *	Hardware type (1)	Hardware address length (1)	Hops (1)
Transaction ID (4)			
Seconds (2)		Flags (2)	
Client IP address (4)			
Your IP address (4)			
Server IP address (4)			
Gateway IP address (16)			
Client hardware address (16)			
Server name (64)			
File name (128)			
Vendor-specific area (64)			
* The number in parentheses indicates the number of octets in each field.			

SNM0001A

Figure 2-6. BOOTREQUEST and BOOTREPLY Fields

The packet relay process uses these fields as follows:

1. When a router interface receives a BOOTREQUEST packet, the router examines the seconds and hops fields in the packet and compares these values to BOOTP parameters you configured on that interface.

   The seconds field contains the minimum number of seconds that the router waits before forwarding a BOOTREQUEST packet. If the value in the seconds field of the packet is less than the value of the Timeout Secs. parameter you configured on the interface, the router drops the packet.

   The hops field contains the maximum number of hops that a packet can take between the source and destination devices. If the packet has traversed more hops than the value of the hops parameter you specified for that interface, the router drops the packet.

2. If the router accepts the packet, it alters the packet by

   - Incrementing the hops field by 1

- Writing the IP address of the input interface to the gateway IP address field

3. The router then determines which networks should receive this packet and broadcasts it to other networks through a forwarding route that you specify when you configure the router for BOOTP services.

   If the BOOTP packet has to travel to a network through another router, you must specify the forwarding route using one of the following methods:

   - Configure the second router for BOOTP services

     In this case, the second router inspects the packet in the same way as the first router, and increments the hops field by 1. The second router will not, however, replace the address in the gateway IP address field, because servers will reply to the first router that received the BOOTREQUEST packet.

   - Configure the first router to forward the BOOTREQUEST packet to a specific server.

     In this case, the router will unicast the BOOTREQUEST packet to the server through normal IP services.

4. Servers on other networks receive the BOOTREQUEST packet and respond with a BOOTREPLY packet. Those servers transmit the BOOTREPLY packets through normal IP services to the address of the first interface that received the BOOTREQUEST packet. That address appears in the gateway IP address field in the BOOTREQUEST packet.

5. When the router that first received the BOOTREQUEST packet receives the BOOTREPLY packet, it examines the gateway IP address field to check that the value in this field is the same as the IP destination address that the server used for the packet. If the addresses differ, the router discards the BOOTREPLY packet.

6. If the router accepts the packet, it examines the flags field and forwards the packet to the client as follows:

   - If the flags field contains the value 1, the client does not know its own IP address. The router broadcasts the BOOTREPLY packets to the IP broadcast address (255.255.255.255).

- If the flags field contains the value 0, the client knows its own IP address, which appears in the client IP address field of the BOOTREPLY packet. The router sends the BOOTREPLY packet to that IP address and the link-layer address that appears in the client hardware address field.

DHCP Overview

DHCP is an extension of BOOTP and is also built on the client-sever model. DHCP provides a method for dynamically assigning IP addresses and configuration parameters to other IP hosts or clients in an IP network. DHCP is specifically designed for servers in large network environments and complex TCP/IP software configurations.

DHCP allows a host to automatically allocate reusable IP addresses and additional configuration parameters for client operation, and allows the client-server host to configure parameters not directly related to the IP protocol. This feature allows the host to exchange packets with any other host on the network.

DHCP enables clients to obtain an IP address for a fixed length of time (a *lease period*) from remote servers (*DHCP servers*). Groups of hosts that do not need permanent IP addresses can lease an address from a limited pool of addresses. The lease period can range from 1 minute to 99 years. When the lease period expires, the server can assign the IP address to another client on the network. DHCP also enables clients to acquire the IP configuration parameters they need to communicate on a network.

The DHCP packet format is based on a BOOTP packet. As a result, DHCP uses the BOOTP relay agent to forward DHCP packets. This scheme provides interoperability between the existing BOOTP clients and DHCP servers. The BOOTP relay agent uses the same criteria and methods for forwarding both DHCP and BOOTP packets. Refer to “BOOTP Relay Agent Overview,” earlier in this chapter, for information about the packet relay process.

Although BOOTP and DHCP use the same UDP port numbers (67 and 68), they differ in the following ways:

- DHCP defines a mechanism for clients to obtain their IP network address for a fixed period of time (lease), allowing for reassignment of expired IP network address to different clients.
- DHCP provides a mechanism for clients to acquire all of the IP configuration parameters needed to communicate on a network.
- DHCP packet length is longer than for BOOTP.

  The additional packet length allows a DHCP server to provide the client with all the IP configuration parameters that it needs to operate.
- DHCP is a more complicated protocol than BOOTP.

  DHCP has seven message types; BOOTP uses only two.

Acquiring a New IP Address and New Configuration Parameters

DHCP acquires an IP address and other configuration parameters for clients. This process involves the following stages:

- Identifying DHCP servers
- Requesting IP information
- Receiving IP information
- Accepting IP information

Figure 2-7 shows the first stage of the process.

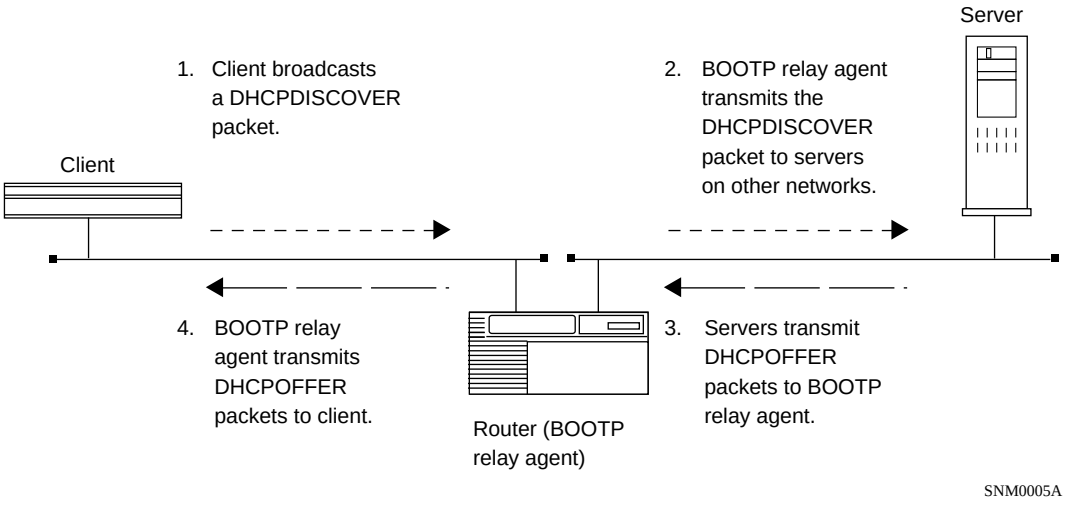
Server
1. Client broadcasts a DHCPDISCOVER packet.
2. BOOTP relay agent transmits the DHCPDISCOVER packet to servers on other networks.
Client
4. BOOTP relay agent transmits DHCPOFFER packets to client.
3. Servers transmit DHCPOFFER packets to BOOTP relay agent.
Router (BOOTP relay agent)
SNM0005A

Figure 2-7. Identifying DHCP Servers

To identify DHCP servers, the client broadcasts a DHCPDISCOVER packet. Figure 2-8 shows the fields in a DHCP packet. The packet relay process uses these fields as follows:

1. A BOOTP relay agent receives the packet, and if it accepts the packet, transmits it to DHCP servers on other networks.

Operation (1) *	Hardware type (1)	Hardware address length (1)	Hops (1)
Transaction ID (4)			
Seconds (2)		Flags (2)	
Client IP address (4)			
Your IP address (4)			
Server IP address (4)			
Gateway IP address (16)			
Client hardware address (16)			
Server name (64)			
File name (128)			
Options (312)			

* The number in parentheses indicates the number of octets in each field.

Figure 2-8. Fields in a DHCP Packet

2. DHCP servers may respond with a DHCPOFFER packet that includes an available IP address in the your IP address field.

   When a DHCP server offers an IP address, that address is temporarily unavailable to other clients. If the client does not accept or reject the address within a certain period of time, the server reclaims it. The address is then available for other clients.

3. The BOOTP relay agent receives the DHCPOFFER packet and examines the packet. If the BOOTP relay agent accepts the packet, it forwards it to the client.

4. If a client does not receive a DHCPOFFER packet within a specified amount of time after broadcasting a DHCPDISCOVER packet, it sends the packet again. The client will rebroadcast the packet up to 10 times.

   The client may receive DHCPOFFER packets from several potential servers. If you configure the client to wait for multiple responses, it compares configuration parameters in the DHCPOFFER packets to decide which server to target.

Figure 2-9 shows the second and third stages of the process.

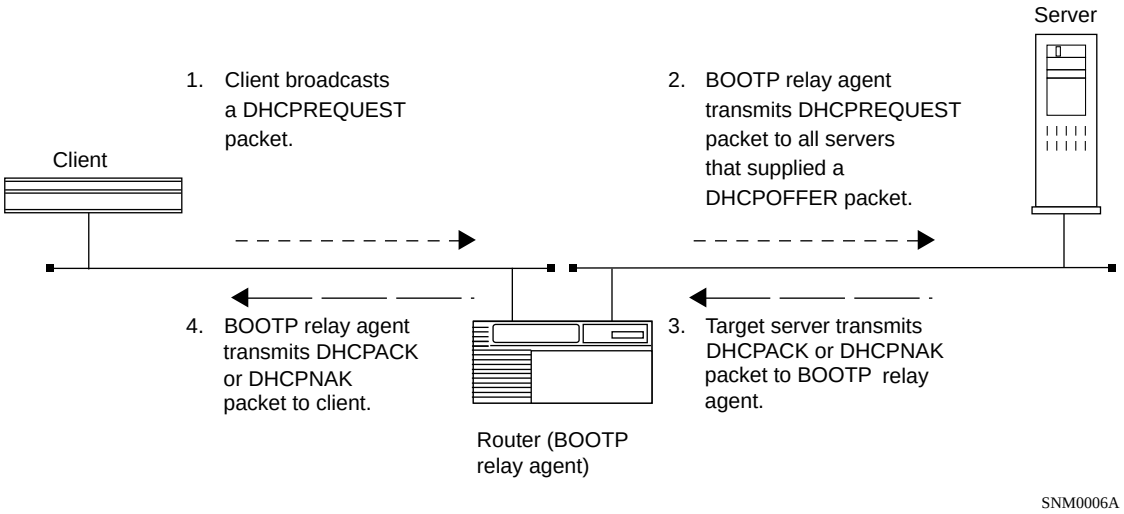
Server
1. Client broadcasts a DHCPREQUEST packet.
2. BOOTP relay agent transmits DHCPREQUEST packet to all servers that supplied a DHCPOFFER packet.
Client
4. BOOTP relay agent transmits DHCPACK or DHCPNAK packet to client.
3. Target server transmits DHCPACK or DHCPNAK packet to BOOTP relay agent.
Router (BOOTP relay agent)
SNM0006A

Figure 2-9. Requesting and Receiving IP Information

5. When the client has chosen a target server, it broadcasts a DHCPREQUEST packet. The DHCPREQUEST packet contains the address of the target server in the server IP address field.

6. The router receives the packet and forwards it to all servers.
7. Those servers examine the packet, and if their IP addresses differ from the value in the server IP address field, they reclaim the IP addresses they supplied in the DHCPOFFER packets. These addresses are now available for other clients.
8. The target server recognizes its IP address in the server IP address field, and responds to the DHCPREQUEST packet as follows:
   - If the target server can supply the requested configuration parameters, it sends a DHCPACK packet to the client through the BOOTP relay agent.

     The client examines the configuration parameters in the DHCPACK packet and records the duration of the lease period. If the client detects a problem with the configuration parameters, it sends a DHCPDECLINE packet to the server and issues a new DHCPDISCOVER packet. Otherwise, the client accepts the configuration parameters.
   - If the target server cannot supply the requested configuration parameters, it sends a DHCPNAK packet to the client through the BOOTP relay agent.

     When the client receives the DHCPNAK packet, it broadcasts a new DHCPDISCOVER packet and the process begins again.

   A client may choose to relinquish its IP address before the lease period expires by sending a DHCPRELEASE packet to the server. This packet contains the relinquished IP address in the client IP address field and the client's MAC address in the client hardware address field.

Acquiring the Same IP Address Again

A client may want to reuse an IP address that a server allocated earlier by DHCP. In this case, the interchange between client and server omits some of the steps described in the previous section, and proceeds as follows:

1. The client starts the interchange by broadcasting a DHCPREQUEST packet that contains its previous IP address in the client IP address field.
2. The BOOTP relay agent forwards the packet to DHCP servers on other networks.
3. DHCP servers examine the client's configuration parameters in the options field of the DHCPREQUEST packet.

4. The server that originally supplied the configuration parameters recognizes them and responds with a DHCPACK packet.
5. When a client receives a DHCPACK packet, it accepts or declines the parameters, as it would when receiving a new IP address.

If a client's request is invalid (for example, if the client has moved to a new network), servers respond with a DHCPNAK packet. If a client receives only DHCPNAK packets, it must request a new IP address by broadcasting a DHCPDISCOVER packet.

RARP Overview

You can use a Bay Networks router as a Reverse Address Resolution Protocol (RARP) server that assigns IP addresses to its clients on the local area network. When you configure a router to use RARP services, it acts as a RARP server. A RARP server supplies clients on the same physical or logical LAN with IP addresses (Figure 2-10).

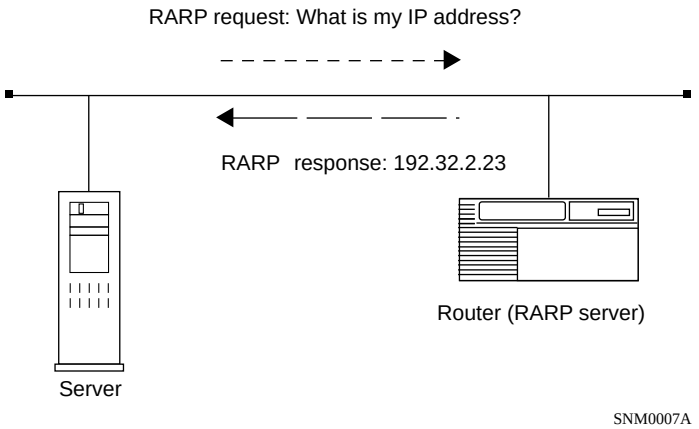

Figure 2-10. RARP Server Supplying an IP Address

To use RARP services, you must set up a MAC address-to-IP address mapping table. This table lists the MAC addresses of clients and the corresponding IP addresses that the RARP server should assign to those clients. When a client needs to acquire an IP address, the following interchange takes place:

1. The client broadcasts a RARP request specifying its MAC address.
2. Upon receiving a RARP request, the router refers to its MAC address-to-IP address mapping table, then sends the client a response packet containing the corresponding IP address.
3. The client examines the response packet to learn its IP address.

You can configure RARP support on Ethernet and Token Ring interfaces, and on the Fiber Distributed Data Interface (FDDI).

Chapter 3
Customizing SNMP

This chapter describes how to customize SNMP services. It assumes you have configured an IP interface using the default parameters, as described in Chapter 1, and that you understand the SNMP concepts in Chapter 2.

You can enable SNMP services most easily by accepting all the default parameter values. However, you may want to change these values, depending on your network requirements. This chapter describes choices you can make to use SNMP most effectively on your network.

Customizing SNMP Global Parameters

After you have enabled SNMP, you can customize SNMP global parameters.

Disabling and Reenabling SNMP

When you enable IP on an interface, SNMP is automatically enabled on that interface and default values are in effect for all SNMP parameters (refer to Appendix B for parameter defaults).

To disable the SNMP agent on all IP interfaces, set the Enable/Disable parameter to Disable. To reenable the SNMP agent on all IP interfaces, set the Enable/Disable parameter to Enable.

Site Manager: Enable parameter: page A-2

Caution: When you disable the SNMP agent in dynamic mode, you immediately prohibit Site Manager from communicating with the router.

Enabling and Disabling SNMP Locking

The SNMP locking mechanism prohibits the SNMP agent from responding to multiple network management stations issuing simultaneous SNMP **set** commands to the router.

The SNMP locking mechanism is enabled by default. This means that the SNMP agent identifies the station from which it receives the next SNMP **set** command and, for a time equal to the value of the Lock TimeOut parameter, responds only to SNMP **set** commands from that station. If the agent receives an SNMP **set** command from another network management station during this time, it issues an SNMP genErr GetResponse PDU, which that station logs as an SNMP SET ERROR message.

To allow the SNMP agent to respond to simultaneous SNMP **set** commands from multiple network management stations, set the SNMP locking mechanism to Disable.

Site Manager: Use Lock parameter: page A-2

Specifying a Lock Timeout Period

If the SNMP locking mechanism is enabled, you can customize the lock timeout period. The lock timeout period is the maximum number of minutes the SNMP agent allows an idle network management station to hold a lock on it. During this time, the SNMP agent locks out SNMP **set** commands from other network management stations. The lock timer is reset each time the locking manager issues an SNMP **set** command.

By default, the SNMP agent allows an idle network management station to hold a lock on it for 2 minutes. To change the default lock timeout period, specify a value from 1 to 60 minutes.

Site Manager: Lock Time Out parameter: page A-3

Enabling and Disabling Authentication Failure Traps

The router generates an authentication failure trap when it receives an SNMP message from an SNMP manager falsely claiming to be in a particular community or specifying an unknown community.

When you enable the authentications failure trap feature on the router, you must configure an SNMP community manager to receive the trap. (Refer to "Configuring SNMP Community Managers," later in this chapter.)

You can prohibit the router from generating authentication failure traps by disabling the authentication failure trap feature.

Site Manager: Authentication Failure Traps parameter: page A-3

Configuring SNMP Community Parameters

An SNMP community is a logical relationship between an SNMP agent and one or more SNMP managers. The community has a name, and all members of a community have the same access privileges: either read-only (members can view configuration and performance information) or read-write (members can view configuration performance information, and also change the configuration).

This section describes how to add and delete the SNMP communities to which the SNMP agent responds or sends traps.

Adding an SNMP Community

When you add an SNMP community, you must specify the name of the community and the access privileges that the router grants to all members of the community.

Specifying a Community Name

Specify a community name that consists of up to 63 characters, including embedded spaces.

Site Manager: Community Name parameter: page A-4

Specifying Community Access Privileges

Specify one of two types of access privileges to each community that you define: read-only or read-write.

By default, the router grants read-only access privileges to all members of an SNMP community. Read-only access allows members of a community to view configuration and performance information. Set this parameter to Read-Write to allow members of a community to view configuration and performance information, and also change the configuration of a router.

Site Manager: Access parameter: page A-4

Deleting an SNMP Community

To delete an SNMP community:

1. **In the Configuration Manager window, select Protocols > IP > SNMP > Communities.**

   The SNMP Community List window opens.

2. **Select the community you want to delete.**

   The Delete Community window opens. Verify that the correct community name appears in the window. Select Cancel if you do not want to delete the selected community.

3. **Click on Delete.**

Configuring SNMP Community Managers

This section describes how to add and delete SNMP community members (managers). It also describes how to configure managers to receive traps from the SNMP agent.

Adding a Manager

After you have added a community name on the router and assigned access privileges to it, you can add specific community members (called *managers)*. You can add more than one manager to a community.

By default, the IP address 0.0.0.0 is a manager in the public community.

Note: When you add the first IP interface, Site Manager automatically creates a read-write public community with a wildcard manager (0.0.0.0). For security reasons, we recommend that you replace the public community and wildcard manager with a unique community specifying a limited list of managers.

To add a manager to a particular community:

1. **In the Configuration Manager window, select Protocols > IP > SNMP > Communities.**

   The SNMP Community List window opens.

2. **Select the community to which you want to add managers.**
3. **Select Community > Managers.**

   The SNMP Manager List window for that community opens.

4. **Select Manager > Add Manager.**

   The Add SNMP Manager window opens.

5. **Enter the IP address of the SNMP manager you want to add.**
6. **Click on OK.**

Configuring a Manager to Receive Traps

After you add a manager to a community, you can configure the manager to receive traps by specifying its UDP port number and the types of traps the agent transmits to that manager.

When you configure a manager to receive specific traps or all traps (refer to Table 3-1), the router sends this manager all enabled event traps. There is no MIB correspondence between a specific SNMP manager and a trap entity. Rather, all SNMP managers that you configure to receive specific traps receive all traps you have configured.

Specifying the Trap Port

By default, the standard port number on the managing station to which the SNMP agent transmits traps is 162. To use a different UDP port number, specify a value from 1 to 9999. Be sure that you do not specify a port that another application uses.

Site Manager: Trap Port parameter: page A-5

Specifying a Trap Type

You can specify one of four types of traps that the SNMP agent can transmit to the manager: Generic, Specific, All, or None.

Table 3-1 describes these four trap options.

Table 3-1. Trap Types Transmitted by the SNMP Agent

Trap Type	Description
Generic	This is the default trap type. It transmits the well-defined SNMP traps (cold-start, warm-start, and authentication failure traps) to the manager. The well-defined, cold-start, and warm-start traps are automatically active in the SNMP agent; however, you must enable the Authentication Failure Traps attribute for the agent to transmit such traps to a specified manager.
Specific	Allows you to configure the agent software to transmit all enabled log event traps to a specified manager.
All	Allows you to transmit cold-start and warm-start traps, and all enabled log event traps to a specified manager.
None	Prohibits the SNMP agent from transmitting traps to a specified manager.

Site Manager: Trap Types parameter: page A-5

Deleting a Manager

You can delete a manager from its associated community by deleting the manager's IP address from the list of SNMP managers.

To delete a manager:

1. **In the Configuration Manager window, select Protocols > IP > SNMP > Communities.**

   The SNMP Community List window opens.

2. **Select the community from which you want to delete the manager.**
3. **Select Community > Managers.**

   The SNMP Manager List window for that community opens.

4. **Select the manager you want to delete.**
5. **Select Manager > Delete Manager.**

   The Delete SNMP Manager window opens.

6. **Make sure the correct manager's IP address appears.**
7. **Click on Delete.**

Configuring Traps on the Router

A *trap* is an event that the router transmits to some external network device, such as a network management station. You can specify which log event traps the SNMP agent sends to the network management station as traps based on the following:

- *Slot number:* the number of the slot on which the trap will be received
- *Entity number*: the code assigned to the entity issuing the event that uniquely identifies a router event
- *Severity level:* indicates whether the trap is a fault, warning, information, trace, or debug message

A router never broadcasts traps on the network. Rather, if sends traps to specific IP addresses, which you configure on the router as managers of a community. Traps are always sent to specific managers.

Specifying a Trap Entity and Severity Level

A trap entity is associated with a log event. An entity is the software that generates a message. Entities include Bay Networks software dedicated to the operation of a software service, such as TFTP and IP. Each entity contains a specific code that corresponds to the event you want to configure.

The entity code, together with the event code, uniquely identifies the event for which you want to configure a trap. For a complete list of entities (both their abbreviations and full names) and associated entity codes, refer to *Event Messages for Routers and BNX Platforms*.

After you specify the number of the slot on which the trap will be received, you specify the entity name for which you want to configure traps.

Trap messages are always associated with one of five severity levels: information, warning, fault, trace, or debug. The severity level defines the type of trap that the SNMP agent sends to the network management station for the slot number and entity type you specified. For a description of the severity levels, refer to *Event Messages for Routers and BNX Platforms.*

To specify a trap entity and the severity level for which you want to receive the trap:

1. **In the Configuration Manager window, select > Protocols > IP > SNMP > Trap Configuration > Interfaces.**

   The Trap Configuration window opens.

2. **Select the slot for which you want to configure traps.**

   You select a slot by clicking on the bar in the Slot box.

3. **Select an entity for which you want to configure traps.**

   The entity names appear in the Available Entities column, a comprehensive list of all protocols available, regardless of the platform or software you are using.

   If you want to configure traps for all entities running on a slot, select All Entities from the top of the column.

4. **Select the severity level for which you want to receive traps.**

   You select a severity level by clicking on the Events box at the bottom of the window. Refer to Chapter 2 for a definition of the severity levels.

5. **Click on Update.**

   The entity name moves to the Current Entities column, indicating that you want to receive traps for this entity at the severity level you specified.

   (To move an entity from this column, select the entity name and then click on Remove.)

6. **Repeat Steps 2 through 5 for other slots you want to configure.**

7. **Click on Save.**

Configuring Trap Exceptions

You can configure up to 50 trap exceptions, which specify that the SNMP agent always sends or never sends traps to the network management station regardless of the trap configuration settings and regardless of the slot you specified.

You configure a trap exception by specifying the following:

- Entity code for the event for which you want to configure an exception
- Code number of the event for which you want to configure an exception
- Whether the SNMP agent always sends or never sends a trap to the network management station

Refer to *Event Messages for Routers and BNX Platforms* for entity codes.

To configure a trap exception:

1. **In the Configuration Manager window, select > Protocols > IP > SNMP > Trap Configuration > Exceptions.**

   The Trap Exceptions List window opens.

2. **Click on Add.**

   The Add Trap window opens.

3. **Specify the entity code and the event code number, and specify Always or Never for the Always/Never Trap parameter.**

4. **Click on OK.**

Site Manager: Entity Code parameter: page A-6
Site Manager: Event Code parameter: page A-6
Site Manager: Always/Never Trap parameter: page A-7

Deleting Trap Exceptions

To delete a trap exception:

1. **In the Configuration Manager window, select Protocols > IP > SNMP > Trap Configuration > Exceptions.**

   The Trap Exceptions List window opens.

2. **Select the trap for which you want to delete the exception.**
3. **Click on Delete.**

Configuring Thresholds

You can configure thresholds for any integer, counter, gauge, or time-tick variable in the MIB. Refer to Chapter 2 for more information about using thresholds.

To configure a threshold, you must have a good understanding of the MIB and be able to identify the instances of MIB objects to which you want to apply a threshold. For complete information about identifying a MIB object or an instance identifier, refer to the statistics section of *Managing Routers and BNX Platforms*.

Disabling and Reenabling Thresholds

By default, the thresholds feature is enabled on all interfaces on which IP is configured. To disable the thresholds feature, set the Enable/Disable parameter to Disable. To reenable the thresholds feature, set the Enable/Disable parameter to Enable.

Site Manager: Enable/Disable parameter: page A-7

Setting the Threshold Polling Interval

The threshold polling interval sets the time interval at which the agent polls the variable to determine whether that variable has reached a threshold. You must set a minimum polling interval of 5 seconds; there is no maximum value. The default polling interval is 60 seconds.

When setting a polling interval, remember that the more often the agent polls the variable, the more memory it needs to manage the thresholds for this statistic.

Site Manager: Polling Interval parameter: page A-8

Adding a Threshold

To add a threshold:

1. **In the Configuration Manager window, select Protocols > Global Protocols > Thresholds > Thresholds.**

   The Thresholds Interface Lists window opens.

2. **Click on Add.**

   The Threshold Configuration window opens, displaying a list of all MIB objects the agent supports.

3. **Select the object to which you want to apply a threshold.**

   The object appears in the Object field.

4. **Enter the instance identifier in the Instance field.**

5. **Click on Save.**

   The Threshold Interface Lists window opens again.

6. **Click on Apply.**

7. **Repeat Steps 2 through 6 to add other thresholds.**

8. **Click on Done when you have finished adding thresholds.**

Enabling and Disabling Thresholds for a Variable

You can decide whether to turn the threshold for a specific variable on or off by specifying the Threshold Enable parameter.

To tell the agent to apply the threshold to a variable, specify Enable. To tell the agent to ignore the threshold for a variable, specify Disable.

Site Manager: Threshold Enable parameter: page A-8

Specifying a Value for the Threshold Level

You can specify an integer value that determines the level (low, medium, or high) at which you want the agent to generate a threshold exception event for a variable.

Site Manager: Threshold Low Value parameter: page A-9
Site Manager: Threshold Medium Value parameter: page A-10
Site Manager: Threshold High Value parameter: page A-11

Specifying the Severity Level for Event Messages

You can specify the severity level of the event message that the agent generates when a variable exceeds either a low, medium, or high threshold level.

You can specify one of three severity levels:

- *Information:* allows low, medium, or high threshold exceptions to generate routine events that require no action
- *Warning:* allows low, medium, or high threshold exceptions to generate events that indicate an unexpected situation occurred
- *Debug:* allows low, medium, or high threshold exceptions to generate events you use to solve network problems

Site Manager: Threshold Low Event Level parameter: page A-9
Site Manager: Threshold Medium Event Level parameter: page A-10
Site Manager: Threshold High Event Level parameter: page A-11

Specifying Threshold Units

You can specify the units used to determine whether a variable has exceeded a threshold.

- To generate a threshold event when the variable's rate of change *per second* reaches one of the three thresholds, set the Threshold Units parameter to Persecond.
- To generate a threshold event when the value of the variable reaches one of the three thresholds, set the Threshold Units parameter to Absolute.

Site Manager: Threshold Units parameter: page A-12

Determining When to Record Threshold Events

You can determine when the agent generates a threshold event by setting the Threshold Action parameter.

By default, the agent generates a threshold event when the value of the variable you specify is *greater than* the threshold you specify. If you want the agent to generate threshold events when the value of the variable is *less than* the threshold you specify, set the Threshold Action parameter to Lessthan.

Site Manager: Threshold Action parameter: page A-12

Specifying Maximum Successive Alarms

A maximum successive alarm represents two or more polling periods when the agent generates an alarm as a result of an exception at the same threshold level.

You can specify an integer to determine the maximum number of successive alarms that the agent generates for a variable. When the agent exceeds the maximum number of alarms, it marks the threshold as held. The agent generates no more alarms until the variable either crosses the threshold at a different level or crosses no threshold for the number of polling intervals equal to the value of the Threshold HoldDown Intervals parameter.

Site Manager: Threshold Max Successive Alarms parameter: page A-13

Specifying Polling Intervals for Held Variables

You can specify an integer value to determine the number of exception-free polling intervals through which a variable in a held state must pass before the variable is no longer considered held. The lower the number you specify, the more likely the agent is to generate repetitive event messages for a variable that is intermittently exceeding thresholds.

Site Manager: Threshold HoldDown Intervals parameter: page A-13

Specifying a Threshold Object Name

By default, the ASN.1 object identifier is the object name that appears in the Threshold Label parameter field. You can replace the ASN.1 object identifier by specifying a name for the object in string format. The string you enter appears in the log file, making it easier to identify the object that is the subject of the trap.

Site Manager: Threshold Label parameter: page A-14

Chapter 4
Customizing a DCM for RMON

This section describes how to customize an Ethernet data collection module (DCM) as a remote monitoring (RMON) device. It also describes how to modify the DCM configuration by changing DCMMW configuration parameters.

This chapter includes the following topics:

- Ethernet DCM and RMON summary
- Managing the Ethernet DCM configuration
- Managing the Ethernet DCM using the Technician Interface
- Viewing and analyzing statistics using Optivity

Refer to Chapter 2 for RMON concepts and the issues you should consider when using an Ethernet DCM for RMON. Refer to Appendix B for DCMMW parameter defaults.

Ethernet DCM and RMON Summary

The Ethernet DCM physically connects to BayStack AN and ANH base modules. It contains a Flash memory SIMM for its own boot image and configuration file. The Ethernet DCM runs RMON agent software that

- Gathers statistics by monitoring packets on an Ethernet segment
- Stores the information according to the RMON MIB specification, in compliance with RFC 1757

To communicate with the RMON agent software on the DCM, the router requires a software subsystem, called *DCM middleware* (DCMMW). This software subsystem enables and configures an installed DCM.

Using Site Manager or the Technician Interface, you configure the DCMMW to

- Enable the Ethernet DCM with a default configuration (refer to Chapter 1)
- Modify the Ethernet DCM configuration
- Boot the Ethernet DCM
- Disable the DCM

Modifying the DCM Configuration

You can modify the DCM configuration on an installed Ethernet DCM by changing the DCMMW configuration parameters.

Before you can change DCMMW configuration parameters for an installed Ethernet DCM, you must temporarily disable the Ethernet DCM from collecting data. When you finish changing the DCMMW configuration parameters, you must reenable the Ethernet DCM for these changes to take effect.

Site Manager: Enable/Disable parameter: page A-14

Specifying the DCM Boot Image Name

By default, the DCM uses the boot image in its own Flash memory for booting. If the Boot Option parameter is set to Download, you must specify a boot image from the ANH Flash memory. The boot image name cannot exceed 255 characters.

To specify the DCM boot image, enter the volume and file name for the image you want the DCM to boot, using the following format:

<*volume_number:filename*>

For example:

1:dcm_image

Site Manager: Image Name parameter: page A-15

Specifying the Boot Option

By default, the DCM uses the image file in DCM local Flash memory as the DCM boot image. If you want the DCM to use an image file on the ANH Flash memory as the DCM boot image, set the Boot Option parameter to Download. When the DCM boots in Download mode, the DCMMW software moves a copy of the image to DCM shared memory. You specify the downloaded image with the Image Name parameter.

If you want the DCM to use the image file in DCM local Flash memory as the DCM boot image, remember to set the Boot Option parameter back to Local.

Site Manager: Boot Option parameter: page A-15

Saving the Boot Image File

By default, the DCM saves the boot image file to its local Flash memory (writing over the existing saved image). If you do not want to save the DCM boot image file (the image remains in DRAM until the next time the DCM boots), set the Image Save Mode parameter to No Save.

Site Manager: Image Save Mode parameter: page A-16

Specifying the Configuration Mode

The configuration mode allows you to specify whether to use configuration information in the DCM Flash memory or in the DCM's shared memory space (DRAM).

To use the default configuration information in the DCM local Flash memory, set the Configuration Mode parameter to Local. To use the configuration information in the DCM DRAM, written by DCMMW from the ANH file system, set the Configuration Mode parameter to Shared Memory.

Site Manager: Configuration Mode parameter: page A-16

Saving the Configuration Information

You can specify whether or not to save the configuration information in DRAM to the DCM Flash memory.

To save the configuration information in DRAM to the DCM Flash memory (writing over the existing configuration file), set the Save Configuration Info parameter to Write. To avoid overwriting the DCM configuration file, set the Save Configuration Info parameter to No Write.

Site Manager: Save Configuration Info parameter: page A-17

Specifying the Maximum Number of RMON Hosts

You can specify the maximum number of host addresses to be collected in each entry of the RMON host control table. The maximum limit depends on the amount of Flash memory available in the DCM. When the host control table reaches the maximum value, the DCM deletes entries based on an LRU (least recently used) algorithm.

The RMON Max Host parameter relates to the RMON Host group.

To verify the number of hosts configured, check the MIB object wfDCMmsRMONHost using the Site Manager Statistics tool.

Site Manager: RMON Max Host parameter: page A-17

Disabling the RMON Host Control Table

By default, the RMON Default Host parameter is enabled, which causes the router to create the RMON host control table each time you boot the Ethernet DCM. Some RMON network management applications expect the Ethernet DCM to set up a host configuration. Others enable and disable their own configurations during normal operations.

You can disable default creation of the RMON host control table at boot time by setting the RMON Default Host parameter to Disable. To re-create the RMON host control table at the next (and every subsequent) reboot, set the RMON Default Host parameter to Enable.

Note that the DCM allows only one instance of the host control table.

Site Manager: RMON Default Host parameter: page A-18

Disabling the RMON Default Matrix Table

Be default, the RMON Default Matrix parameter is enabled, which causes the router to create the RMON matrix control table each time you boot the Ethernet DCM. Some RMON network management applications expect the Ethernet DCM to set up a matrix configuration. Others enable and disable their own configurations during normal operations.

You can disable default creation of the RMON matrix control table at boot time by setting the RMON Default Matrix parameter to Disable. To re-create the RMON matrix control table at the next (and every subsequent) reboot, set the RMON Default Matrix parameter to Enable.

Note that the DCM allows only one instance of the matrix control table.

Site Manager: RMON Default Matrix parameter: page A-18

Rebooting the Ethernet DCM

After you finish modifying the DCM configuration parameters, you must reboot the Ethernet DCM for these changes to take effect. You do this by reenabling the Ethernet DCM if it is in a disabled state.

Site Manager: Enable/Disable parameter: page A-14

Deleting the Ethernet DCM Software Subsystem

The router requires the DCMMW software to communicate with the Ethernet DCM. Deleting DCMMW deactivates the Ethernet DCM.

Note: Always try disabling the Ethernet DCM by setting the Enable/Disable parameter to Disable before you delete the DCMMW software.

To completely deactivate the Ethernet DCM:

1. **In the Configuration Manager window, select Platform > DCM 11.0 and later > Delete... > Base Module DCM only.**

   The Configuration Manager displays a confirmation prompt.

2. **Click on OK.**

   The Configuration Manager deletes the DCMMW base record, bringing the Ethernet DCM completely down.

After deleting the Ethernet DCM configuration, you can reactivate the Ethernet DCM by selecting Platform > DCM 11.0 and later > Create Base Module DCM to re-create the DCMMW record.

Managing a DCM Using the Technician Interface

You can use the Technician Interface commands to

- Download a new Ethernet DCM software image

  Refer to *Upgrading Routers from Version 7-10.xx to Version 11.0* for information about using the **dcmload** script.

- Display or modify DCMMW configuration parameters

  Refer to *Using Technician Interface Scripts* for information about accessing the DCM MIB using **set, get,** and **commit** command with the MIB object ID.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

- Enable, disable, and reboot the Ethernet DCM

  Refer to *Using Technician Interface Scripts* for information about using the **enable/disable dcmmw** scripts.

Caution: Avoid running scripts that continually issue Technician Interface commands while you are running another RMON network management application. This combination can cause the SNMP agent to fill the system buffers with RMON data, causing a system restart.

Viewing and Analyzing Statistics Using Optivity

Once you have enabled the DCM on a BayStack AN or ANH router and the DCM is collecting Ethernet statistics, you can use Optivity Analysis and Optivity LAN software to view, analyze, and monitor network statistics.

Using Optivity Analysis with RMON

Optivity Analysis is a set of graphical network management applications based on RMON. These Optivity applications offer powerful RMON-based tools that work together to keep your network working optimally.

Each RMON tool is a complete application. After the tool requests and receives information from the network management station if processes the information and displays a graphical summary of network traffic. Each tool is configurable, so you can obtain exactly the type of information you need for a variety of purposes.

In Optivity Analysis, RMON tools represent an intelligent implementation of the RMON MIB groups. Table 4-1 summarizes the RMON-based tools and lists the corresponding RMON MIB groups that they use to collect and present traffic statistics.

Table 4-1. Optivity Analysis RMON-based Tools

Tool Name	Purpose	Possible Uses	Special Features	RMON MIB Group
Segment Statistics	Displays and records information from the RMON statistics group. This information includes raw packet counts and bandwidth utilization.	Plan bandwidth-intensive tasks Baseline individual segment traffic characteristics	Ability to view multiple sessions Automatic utilization calculation based on available bandwidth History collection	Ethernet Statistics
Host Statistics	Displays traffic summaries for each host on a selected segment. Provides a Host TopN filter that allows you to concentrate on only the most active hosts on the network.	Determine which hosts are generating specific types of traffic	Filter for viewing TopN hosts Hotlink packet capture	Host Table and Host TopN
Host Matrix	Presents statistics on conversations between host pairs on a selected segment.	Isolate sources of broadcasts, errors and so forth Locate work groups for segmentation	Sparse matrix display Quick view of graphic coding of information Level 3 support for conversations by protocol Hotlink capture	Matrix

(continued)

Table 4-1. Optivity Analysis RMON-based Tools *(continued)*

Tool Name	Purpose	Possible Uses	Special Features	RMON MIB Group
Filter/Capture	Define channels and filters. Activate channels for captures.	Capture packets for analysis of a specific problem or to provide selective traffic statistics.	Flexible channel and filter editors Realtime display of counters Automatic capture activation from other tools	Filter and Packet Capture
DecodeMan	Decode and display captured packet content.	Troubleshoot problems by pinpointing the source	Full seven-layer decode Quick search index Quick configuration of RMON probes for standalone operation	Filter and Packet Capture
Alarm Editor	View thresholds for segment. Run Learning Tool locally.	Modify individual normative models Run Learning Tool with local configuration for specific segment	Editing of individual thresholds and hysteresis values interactively	Ancillary to Alarm and Events
Alarm Monitor	Continually monitor all segments.	Proactive maintenance	Monitors all segments at once Quick filter by segment or alarm type Hotlink to Filter/Capture and DecodeMan	Alarms and Events
Learning Tool	Automatically “learn” normal network behavior on all segments.	Create normative model comprising threshold values for all segments	Learns automatically Flexible sample Builds model statistically	Ancillary to Alarms and Events

For detailed information about how to install, configure and customize the RMON-based tools for use with RMON, refer to *Using Optivity Analysis 7.0*.

Using Optivity LAN with RMON

Optivity LAN offers two tools you can use to monitor network statistics collected by the Ethernet DCM: Threshold Manager and Fault Correlator. These tools allow you to set thresholds on integer-based RMON objects and display trap information when the threshold is exceeded.

Threshold Manager Tool

After you establish a level of performance that you consider normal for your network, you can set up your system to generate responses whenever your network performance becomes abnormal.

As well as generating fault information, you can set thresholds that initiate alarms whenever specified unfavorable network conditions occur. Whenever a threshold is met or exceeded, the specified event occurs and the alarm is triggered. The Optivity application allows you to set thresholds specific to a slot or port.

With Threshold Manager, you can perform the following network management tasks:

- Display thresholds
- Add, delete, and modify thresholds
- Define custom thresholds on any MIB object (RMON only)
- Save and load thresholds to and from a file
- Save thresholds to nonvolatile random-access memory (NVRAM) (RMON only)

For detailed information about installing the Threshold Manager tool, refer to *Using Optivity Analysis 7.0*.

Fault Correlator Tool

After you set alarm thresholds on RMON variables using the Threshold Manager, you can use the Fault Correlator tool to decode the traps that are sent to the network management station.

The Fault Correlator generates fault reports and calculates the current state of network objects and devices. It generates fault reports by reducing network faults and traps into network problems. Optivity automatically stores this information in the Optivity fault database.

When you boot the management station, the system starts Fault Correlator. Fault Correlator automatically assigns a health status to all network devices and builds an internal model of the network using information from the SuperAgent's domain database and incoming traps.

When a network device or other application receives a trap, the Fault Correlator uses the network model to determine which devices are related to the event. It determines the severity of the event by comparing the trap to the predefined fault and state rules.

For detailed information about using the Fault Correlator tool, refer to *Starting and Using Optivity Internetwork 7.1*.

Chapter 5
Customizing BOOTP

Specifying Maximum Number of Hops from Client to Server

A hop is the logical distance between two devices. By default, the maximum number of hops a packet can take from the source device to the destination device (client to the server) is 4. To change the default, specify a value from 1 to 16.

If the value in the hops field of a BOOTPREQUEST packet is greater than the value you specify for the Hops parameter, the router drops the packet.

Site Manager: Hops parameter: page A-19

Specifying a Minimum Timeout Value

By default, the router immediately forwards BOOTREQUEST packets to the destination address in the BOOTP relay forwarding table. You can determine the minimum number of seconds that the router waits before forwarding a BOOTREQUEST packet out an interface by assigning a value to the Timeout Secs. parameter. If the value in the seconds field of a BOOTREQUEST packet is less than the value you specified for the Timeout Secs. parameter you configured on the interface, the router drops the packet.

The default value is 0 seconds. To change the default, specify a value from 1 to 65535 seconds.

Site Manager: Timeout Secs. parameter: page A-20

Filtering Unwanted BOOTP and DHCP Packets

Both BOOTP and DHCP use the BOOTP relay agent to forward packets. To reduce network traffic, you may want to control whether an interface transmits BOOTP packets, DHCP packets, or both. For example, you may want to set a filter to prevent BOOTP traffic from traversing a network segment that contains DHCP servers but not BOOTP servers.

You configure this type of filter by setting the Pass Through Mode parameter. The default setting is BOOTP and allows the interface to transmit only BOOTP packets. Be sure to change the setting if you want to transmit DHCP messages.

Site Manager: Pass Through Mode parameter: page A-20

Setting Up the Routing Path between the BOOTP Server and the Routers

You must define the routing path between the BOOTP server and the routers to ensure the successful transmission of BOOTREQUEST packets from one end of the network to the other. You define this routing path by

- Enabling BOOTP forwarding on upstream routers
- Creating a BOOTP relay agent forwarding table for each router in the path

Enabling BOOTP on Router Interfaces

Before you enable BOOTP on router interfaces, make sure that the router is in forwarding mode. Setting the router to forwarding mode allows the BOOTP relay agent to route (forward) all BOOTREQUEST packets and to process both broadcast packets and all packets explicitly addressed to it. For instructions on configuring the router in forwarding mode, refer to *Configuring IP Services*.

You must enable BOOTP (also called BOOTP pass-through or gateway) on all interfaces in the paths between the routers and the BOOTP server. For example, you would enable BOOTP on the interfaces indicated in Figure 5-1.

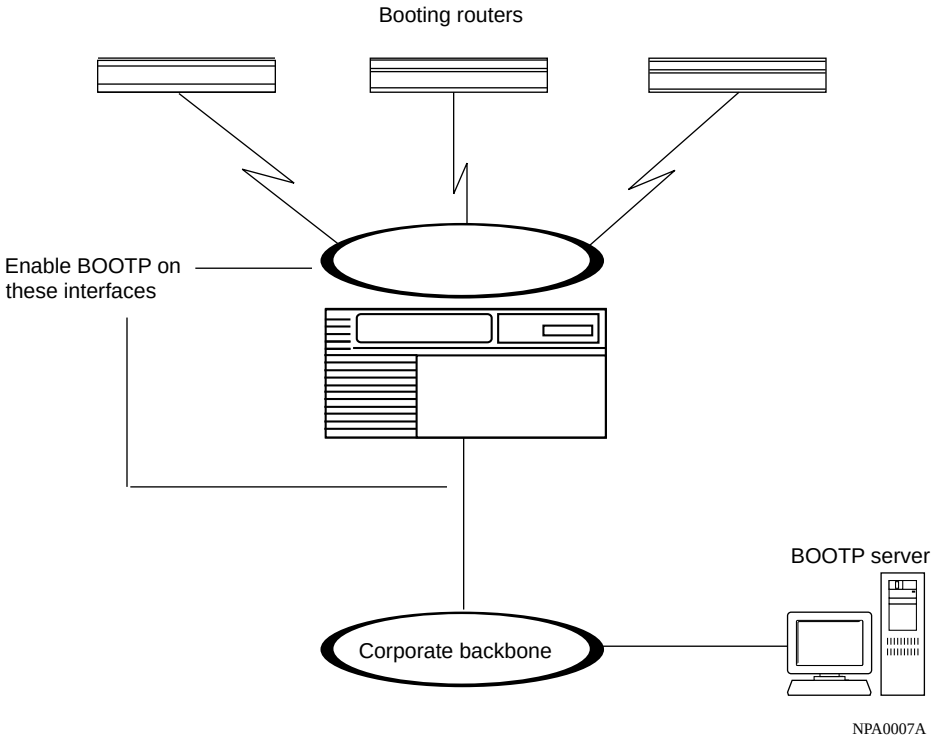

Figure 5-1. Enabling BOOTP in a Sample Network

To enable BOOTP on an interface:

1. **In the Configuration Manager window, click on the connector.**

   The Edit Connector window opens.

2. **Select Edit Circuit.**

   The Circuit Definition window opens.

3. **Select Protocols > Add.**

   The Select Protocols window opens.

4. **Select BOOTP.**

5. **Click on OK.**

6. **Select File > Exit to exit the Circuit Definition window.**

Specifying Interfaces to Receive and Relay BOOTREQUEST Packets

You can specify a forwarding route for BOOTREQUEST packets by defining a relationship between an interface you want to receive BOOTREQUEST packets and another to transmit BOOTREQUEST packets. When you define this type of relationship, the interface pair appears in the BOOTP relay agent forwarding table.

Depending on the configuration of your network, you can specify

- One input IP interface to forward packets to multiple output IP interfaces
- Multiple input interfaces to forward to multiple output interfaces
- Multiple input interfaces to forward to one output interface

Creating a BOOTP Relay Agent Forwarding Table

You must create a BOOTP relay agent forwarding table for every transient router passing BOOTP traffic between a router and the BOOTP server.

The BOOTP relay agent forwarding table consists of IP interfaces that you configure to receive the incoming BOOTP request packets and to forward the outgoing BOOTP request packets. The BOOTP relay agent forwards BOOTP request packets based on the IP addresses of the interfaces in this table. You can add multiple pairs of incoming and outgoing interfaces to support connections to multiple routers in your network. For more information about configuring a forwarding table, refer to *Configuring IP Services.*

Specifying the IP Interface Input/Output Address Pair

You create the BOOTP relay agent forwarding table by specifying the IP interface addresses (input and output) of the pair that you want to receive and forward BOOTREQUEST packets. If you enter an IP address that you have not configured on the router, `???` appears before the IP address (example: `??? 111.111.111.111`). When you configure the IP address on the router, Site Manager replaces `???` with the appropriate address.

Do not specify an unnumbered interface for the input or output IP interface address parameters. If you want to use an unnumbered interface to transmit BOOTREQUEST or DHCP packets to the servers, you must set up a preferred server in the BOOTP Relay Agent Interface Table window (refer to "Configuring BOOTP Preferred Servers," later in this chapter).

Site Manager: Input IP Address parameter: page A-21
Site Manager: Output IP Address parameter: page A-21

Deleting an IP Interface Input/Output Address Pair

To delete an input/output address pair from the BOOTP relay agent forwarding table:

1. **In the Configuration Manager window, select Protocol > IP > BOOTP > Relay Agent Interface Table.**

   The BOOTP Relay Agent Interface Table window opens.

2. **Click on Forward I/F.**

3. **In the BOOTP Relay Agent Interface Table window, click on Forward I/F.**

   The BOOTP Relay Agent Forwarding Table window opens.

4. **Select the address pair you want to delete.**

5. **Click on Delete.**

   The BOOTP Relay Agent Forwarding Table window no longer displays the address pair.

6. **Click on Done to exit the window.**

Disabling BOOTP Route Forwarding

By default, the route (interface) through which the router forwards BOOTP or DHCP packets to servers on the network is enabled. You can disable BOOTP or DHCP packet forwarding through this route by setting the Enable/Disable parameter to Disable.

Site Manager: Enable/Disable parameter: page A-22

Configuring an AN to Use EZ-Install over a Frame Relay PVC

If you intend to configure an AN router to use EZ-Install over a Frame Relay PVC in group access mode, you must create a BOOTP *client interface table.* You do not need to create this table if you configured the Frame Relay PVC to operate in direct access mode.

The BOOTP client interface table allows you to specify and pair the IP address of a remote AN router with the DLCI of its Frame Relay group access PVC.

The *upstream router* is a booting router's next-hop router. By default, the booting router's synchronous interfaces automatically try to get IP addresses from the upstream router. This is the EZ-Install process.

If a router using EZ-Install gets its address from the upstream router, and the upstream router's interface to that router is a Frame Relay group access PVC, you must connect to the upstream router and create a BOOTP client interface table (in addition to a BOOTP relay agent forwarding table).

For information about configuring an AN to use EZ-Install, refer to *Installing and Operating BayStack AN and ANH Systems*. For information about DLCIs and Frame Relay, refer to *Configuring Frame Relay Services*.

Creating a BOOTP Client Interface Table

You create a BOOTP client interface table by specifying the client IP address and the Frame Relay PVC DLCI number.

Specifying the Client IP Address

You must specify the IP address of the remote AN router that will boot using EZ-Install over a Frame Relay group access PVC connection to the router.

Site Manager: IP Address parameter: page A-23

Specifying the DLCI Number

You must specify in decimal format the Frame Relay PVC identification number whose destination is the remote AN that will boot using EZ-Install. Use the DLCI number assigned by your Frame Relay service provider. The Frame Relay network uses the DLCI number to direct data flow.

Site Manager: DLCI Number parameter: page A-23

Specifying Servers for BOOTP Services

You can specify a forwarding route for BOOTREQUEST packets by defining a relationship between an input interface and a BOOTP server. By defining such a relationship, you can

- Improve the efficiency of BOOTREQUEST packet relay
- Transmit BOOTREQUEST packets through unnumbered output interfaces

Configuring BOOTP Preferred Servers

You can configure a BOOTP preferred server by specifying the IP address of the relay agent on the router and the IP address of the target server. The router can then unicast a BOOTREQUEST packet through normal IP services to that server.

Specifying the Relay Agent IP Address

You must specify the IP address of a numbered network interface that you want to receive BOOTREQUEST or DHCP packets from clients. You can then configure this IP address on the router, if you have not already done so.

Do not specify an unnumbered interface for this parameter.

Site Manager: Relay Agent IP Address parameter: page A-24

Specifying the Target Server IP Address

After you specify the relay agent IP address, you must specify the IP address of the server that should receive the BOOTREQUEST or DHCP packet from the relay agent.

Site Manager: Target Server IP Address parameter: page A-24

Specifying the Target Server's Host Name

If you want to keep track of the names of BOOTP and DHCP servers, specify the target server's host name. The host name cannot exceed 63 ASCII characters, including embedded spaces.

Site Manager: Target Name parameter: page A-25

After you specify the IP address and host name of the target server, the BOOTP Relay Agent Preferred Server Table window shows the address pair you added and default values for the Enable/Disable and Pass Through Mode parameters.

Disabling the Forwarding Route

By default, BOOTP and DHCP forwarding is enabled for the route that you configured. You can disable BOOTP or DHCP forwarding on this route, if you choose, by setting the Disable/Enable parameter to Disable.

Site Manager: Enable/Disable parameter: page A-25

Filtering BOOTP and DHCP Packets

You can control whether an interface transmits BOOTP packets, DHCP packets, or both to a server by configuring filters for these specific packets. You configure this type of filter by setting the Pass Through Mode parameter in Site Manager. The default setting is BOOTP and allows the interface to transmit only BOOTP packets. Be sure to change the setting if you want to transmit DHCP messages.

Site Manager: Pass Through Mode parameter: page A-25

Deleting the BOOTP Relay Agent from an IP Interface

To delete a BOOTP relay agent from an IP interface:

1. **In the Configuration Manager window, select Protocols > IP > BOOTP > Relay Agent Interface Table.**

   The BOOTP Relay Agent Interface window opens.

2. **Click on the interface from which you want to delete BOOTP.**

3. **Click on Delete.**

   This action deletes the BOOTP relay agent and all forwarding table entries that you specified from the selected interface.

Deleting BOOTP Globally

To globally delete BOOTP from all interfaces on a router:

1. **In the Configuration Manager window, select Protocols > IP > BOOTP > Delete.**

2. **Click on Delete.**

   This action deletes BOOTP from all interfaces on the router.

Chapter 6
Customizing DHCP

This chapter describes how to customize DHCP services. It assumes you have configured an IP interface using the default parameters and enabled DHCP, as described in Chapter 1, and that you understand the DHCP concepts in Chapter 2.

When you enable DHCP, all default parameter values are automatically enabled on that interface (refer to Appendix B for default parameters). You may want to change these default values, depending on your network requirements. This chapter describes choices you can make to use DHCP most effectively on your network.

Customizing DHCP Parameters

After you have enabled DHCP services on a router (refer to Chapter 1), you can customize the router software for your specific requirements. Use the remaining sections in this chapter as a guide.

Specifying Interfaces to Receive and Relay DHCP Packets

You must specify a forwarding route for DHCP packets by defining a relationship between an interface you configure to receive DHCP packets and an interface you want to transmit DHCP packets. When you define this type of relationship, the interface pair appears in the BOOTP relay agent forwarding table. Refer to "Specifying Interfaces to Receive and Relay BOOTREQUEST Packets" in Chapter 5 for instructions.

To allow DCHP operation, be sure to set the Pass Through Mode parameter in the BOOTP Relay Agent Forwarding Table window to DHCP, or to BOOTP and DHCP.

Site Manager: Pass Through Mode parameter: page A-22

Specifying Servers for DHCP Services

You can improve the efficiency of the packet forwarding process or transmit DHCP packets through unnumbered interfaces by specifying servers for DHCP services. Refer to “Specifying Servers for BOOTP Services” in Chapter 5 for instructions.

To allow DHCP operation, be sure to set the Pass Through Mode parameter in the BOOTP Relay Agent Preferred Server Table window to DHCP, or to BOOTP and DHCP.

Site Manager: Pass Through Mode parameter: page A-25

Deleting DHCP from an IP Interface

To delete DHCP from an IP interface, while maintaining BOOTP on that interface, set the Pass Through Mode parameter in the BOOTP Relay Agent Interface Table window to BOOTP.

Site Manager: Pass Through Mode parameter: page A-22

To delete both DHCP and BOOTP from an IP interface, delete the BOOTP relay agent on that interface. Refer to “Deleting the BOOTP Relay Agent from an IP Interface” in Chapter 5 for instructions.

Deleting DHCP Globally

To delete DHCP globally, you must delete BOOTP globally. Refer to “Deleting BOOTP Globally” in Chapter 5 for instructions.

Chapter 7
Customizing RARP

This chapter describes how to customize RARP services. It assumes you have configured an IP interface using the default parameters and enabled RARP services, as described in Chapter 1, and that you understand the RARP concepts in Chapter 2.

You can enable RARP services most easily by accepting all the default parameter values. However, you may want to change these values, depending on your network requirements. This chapter describes the choices you can make to use RARP most effectively on your network.

Customizing RARP Parameters

After you have enabled RARP services on your router (refer to Chapter 1), you can customize the router software for your specific requirements. Use the remaining sections in this chapter as a guide.

Disabling and Reenabling RARP Interfaces

You can disable or reenable individual RARP interfaces by selecting them from a list of interfaces in the RARP Interface Table.

Site Manager: Enable/Disable parameter: page A-26

Defining the RARP Mapping Table

The RARP mapping table lists the clients on the network that use the router's RARP services. You define the router's MAC address-to-IP address RARP mapping table by specifying the MAC addresses of clients and the corresponding IP addresses that the RARP server assigns to those clients.

Specifying the Client's MAC Address

You must specify the MAC address of a client that will use the RARP services of this router. The client will include the MAC address you specify here in RARP broadcasts to the router.

Site Manager: MAC Address parameter: page A-26

Specifying the Client's IP Address

You must specify the IP address corresponding to the value of the MAC Address parameter you specify. Do not accept the default value.

When the router receives a RARP request from the client, it assigns this IP address to the client and includes it in a response packet.

Site Manager: IP Address parameter: page A-27

Disabling RARP Globally

To globally disable RARP from all router interfaces on which it is configured:

1. **In the Configuration Manager window, select Protocols > IP > Reverse ARP > Globals.**

   The Edit RARP Global Parameters window opens.

2. **Set the Enable/Disable parameter to Disable.**

3. **Click on OK.**

   This action disables RARP on all router interfaces.

Deleting RARP Globally

To globally delete RARP from all router interfaces on which it is configured:

1. **In the Configuration Manager window, select Protocols > IP > Reverse ARP > Delete RARP.**

   A confirmation window opens.

2. **Click on OK.**

   This action deletes RARP from all interfaces on the router.

Appendix A
SNMP, DCM, BOOTP, DHCP, and RARP Parameter Descriptions

This appendix provides information about customizing the parameters for the SNMP, DCM, BOOTP, DHCP, and RARP interfaces you configure on the router. For each parameter, this appendix provides the path, the default setting, all valid parameter options, the parameter function, instructions for setting the parameter, and the management information base (MIB) object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify the validity of your parameter values. Entering an invalid value can corrupt your configuration.

SNMP Global Parameters

Use the following guidelines to configure SNMP global parameters in the Configuration Manager window.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > SNMP > Global

Default: Enable

Options: Enable | Disable

Function: Specifies the state of the SNMP agent on all interfaces that support IP.

Instructions: Select Enable to enable the SNMP agent; select Disable to disable the SNMP agent.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.1

Parameter: Use Lock

Path: Configuration Manager > Protocols > IP > SNMP > Global

Default: Enable

Options: Enable | Disable

Function: Specifies whether the agent responds to multiple network management stations issuing simultaneous SNMP **set** commands to the router. When you set this parameter to Enable, the agent identifies the station from which it receives the next SNMP **set** command and, for a time equal to the value of the Lock TimeOut parameter, responds only to SNMP **set** commands from that station. If the agent receives an SNMP **set** command from another network management station during this time, it issues an SNMP genErr GetResponse PDU, which that station logs as an SNMP SET ERROR message.

Instructions: Select Enable to prohibit the agent from responding to simultaneous SNMP commands from multiple network management stations.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.2

Parameter: **Lock Time Out**

Path: Configuration Manager > Protocols > IP > SNMP > Global

Default: 2 minutes

Options: 1 to 60 minutes

Function: Specifies the maximum number of minutes the agent allows an idle network management station to hold a lock on it. During this time, the agent locks out SNMP **set** commands from other network management stations. The lock timer is reset each time the locking manager issues an SNMP **set** command.

Instructions: Enter the number of minutes only if you set the Use Lock parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.4

Parameter: **Authentication Failure Traps**

Path: Configuration Manager > Protocols > IP > SNMP > Global

Default: Enable

Options: Enable | Disable

Function: Specifies whether the router attempts to generate an authentication failure trap when it receives an SNMP message from an SNMP manager falsely claiming to be in a particular community or specifying an unknown community.

Instructions: Select Enable to enable the router to generate authentication failure traps. If you select Enable, you must configure an SNMP manager to receive the trap. You configure a trap in the Trap Configuration window.

Select Disable to prohibit the router from generating authentication failure traps.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.35

SNMP Community Parameters

Use the following guidelines to configure SNMP community parameters in the SNMP Community window.

Parameter: Community Name

Path: Configuration Manager > Protocols > IP > SNMP > Communities > Community > Add Community | Edit Community

Default: None

Options: Any string of printable ASCII characters, up to 63 characters in length, including embedded spaces

Function: Specifies the name of the SNMP community.

Instructions: Enter the SNMP community name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.2.1.3

Parameter: Access

Path: Configuration Manager > Protocols > IP > SNMP > Communities > Community > Add Community | Edit Community

Default: Read Only

Options: Read Only | Read-Write

Function: Specifies the access privileges that the router grants to all members of this SNMP community.

Instructions: Select Read Only to allow members of this community to only view configuration and performance information about this router.

Select Read-Write to allow members of this community to both view configuration and performance information about this router and to change the router's configuration.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.2.1.4

SNMP Manager Parameters

Use the following guidelines to configure SNMP manager parameters in the SNMP Manager window.

Parameter: Trap Port

Path: Configuration Manager > Protocols > IP > SNMP > Communities > Community > Managers > Manager > Add Manager | Edit Manager

Default: 162

Options: 1 to 9999

Function: Specifies the number of the port on the management station to which the agent sends traps.

Instructions: The standard port number for trap messages is 162; however, you may enter a different port number. Be sure not to specify a port that another application uses.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.3.1.5

Parameter: Trap Types

Path: Configuration Manager > Protocols > IP > SNMP > Communities > Community > Managers > Manager > Add Manager | Edit Manager

Default: Generic

Options: None | Generic | Specific | All

Function: Specifies the type of trap the agent sends to this manager.

Instructions: Select None to prohibit the agent from sending traps to this manager.

Select Generic to configure the agent to send the well-defined SNMP traps (cold-start, warm-start, and authentication failure traps) to the manager. The well-defined cold-start and warm-start traps are automatically active in the SNMP agent; however, you must enable the Authentication Failure Traps global parameter for the agent to send such traps to this manager.

Select Specific to configure the agent software to send all enabled log event traps to this manager.

Select All to send cold-start traps, warm-start traps, and all enabled log event traps to this manager.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.3.1.5

SNMP Trap Interface Parameters

Use the following guidelines to configure SNMP trap interface parameters in the Add Trap window.

Parameter: Entity Code

Path: Configuration Manager > Protocols > IP > SNMP > Trap Configuration > Exceptions > **Add**

Default: None

Options: Any valid entity code

Function: Specifies the entity code for the event for which you want to configure an exception.

Instructions: Enter the entity code for the event for which you want to configure an exception. Refer to *Event Messages for Routers and BNX Platforms* for entity codes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.6.1.3

Parameter: Event Code

Path: Configuration Manager > Protocols > IP > SNMP > Trap Configuration > Exceptions > **Add**

Default: None

Options: Any valid event code number

Function: Specifies the code number for the event for which you want to configure an exception.

Instructions: Enter the event code number for the event for which you want to configure an exception. Refer to the book *Event Messages for Routers and BNX Platforms* for event code numbers.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.6.1.4

Parameter: **Always/Never Trap**

Path: Configuration Manager > Protocols > IP > SNMP > Trap Configuration > Exceptions > **Add**

Default: None

Options: Always | Never

Function: Specifies whether the SNMP agent always sends or never sends this trap to the network management station. The instructions you specify in this field override the settings in the Trap Configuration window, and affect traps sent from every slot in the router.

Instructions: Select Always or Never.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.6.1.2

SNMP Threshold Global Parameters

Use the following guidelines to configure SNMP threshold global parameters in the Edit Thresholds Global Parameters window.

Parameter: **Enable/Disable**

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Global

Default: Enable

Options: Enable | Disable

Function: Enables or disables the threshold feature on a router.

Instructions: Select Enable to enable thresholds. Select Disable to disable thresholds.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.1.1

Parameter:	**Polling Interval**
Path:	Configuration Manager > Protocols > Global Protocols > Thresholds > Global
Default:	60 seconds
Options:	5 seconds minimum; no maximum value
Function:	Sets the time interval at which the agent polls the variable to determine whether that variable has reached the threshold.
Instructions:	Specify the number of seconds for the polling interval. Remember that the more often the agent polls the variable, the more memory it needs to manage the thresholds for this statistic.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.1.2

SNMP Threshold Interface Parameters

Use the following guidelines to configure SNMP threshold interface parameters in the Thresholds Interface Lists window.

Parameter:	**Threshold Enable**
Path:	Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds
Default:	Enable
Options:	Enable | Disable
Function:	Turns the threshold for this variable on and off.
Instructions:	Select Enable if you want the agent to apply the threshold to this variable. Select Disable if you want the agent to ignore the threshold for this variable.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.2

Parameter: Threshold Low Value

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: 0

Options: Any integer value

Function: Sets the value of the low threshold for this variable.

Instructions: Specify the level at which you want the agent to generate a low-threshold exception event.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.5

Parameter: Threshold Low Event Level

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: Info

Options: Info | Warning | Debug

Function: Specifies the severity level of the event message the agent generates when a variable exceeds the low threshold.

Instructions: Select Info if you want low-threshold exceptions to generate routine events that require no action.

Select Warning if you want low-threshold exceptions to generate events that indicate an unexpected situation occurred.

Select Debug if you want low-threshold exceptions to generate events you use to solve network problems.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.6

Parameter: Threshold Medium Value

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: 0

Options: Any integer value

Function: Sets the value of the medium threshold for this variable.

Instructions: Specify the level at which you want the agent to generate a medium-threshold exception event.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.7

Parameter: Threshold Medium Event Level

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: Info

Options: Info | Warning | Debug

Function: Specifies the severity level of the event message the agent generates when a variable exceeds the medium threshold.

Instructions: Select Info if you want medium-threshold exceptions to generate routine events that require no action.

Select Warning if you want medium-threshold exceptions to generate events that indicate an unexpected situation occurred.

Select Debug if you want medium-threshold exceptions to generate events you use to solve network problems.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.8

Parameter: Threshold High Value

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: 0

Options: Any integer value

Function: Sets the value of the high threshold for this variable.

Instructions: Specify the level at which you want the agent to generate a high-threshold exception event.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.9

Parameter: Threshold High Event Level

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: Info

Options: Info | Warning | Debug

Function: Specifies the severity level of the event message the agent generates when a variable exceeds the high threshold.

Instructions: Select Info if you want high-threshold exceptions to generate routine events that require no action.

Select Warning if you want high-threshold exceptions to generate events that indicate an unexpected situation occurred.

Select Debug if you want high-threshold exceptions to generate events you use to solve network problems.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.10

Parameter: Threshold Units

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: Persecond

Options: Persecond | Absolute

Function: Specifies the units used to determine whether a variable has exceeded a threshold.

Instructions: Select Persecond if you want the agent to generate a threshold event when the variable's rate of change *per second* reaches one of the three thresholds.

Select Absolute if you want the agent to generate a threshold event when the value of the variable reaches one of the three thresholds.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.12

Parameter: Threshold Action

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: Greaterthan

Options: Greaterthan | Lessthan

Function: Specifies when the agent generates a threshold event.

Instructions: Select Greaterthan if you want to record threshold events when the value of the variable is *greater than* the threshold specified.

Select Lessthan if you want to record threshold events when the value of the variable is *less than* the threshold specified.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.13

Parameter: Threshold Max Successive Alarms

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: 5

Options: Any integer value

Function: Specifies the maximum number of successive alarms that the agent generates for this variable. A successive alarm represents two or more polling periods when the agent generates an alarm as a result of an exception at the same threshold level.

Instructions: Specify the maximum number of successive alarms. When the agent exceeds the maximum number of alarms, it marks the threshold as held. The agent generates no more alarms until the variable either crosses the threshold at a different level or crosses no threshold for the number of polling intervals equal to the value of the Threshold HoldDown Intervals parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.14

Parameter: Threshold HoldDown Intervals

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: 1

Options: Any integer value

Function: Specifies the number of exception-free polling intervals through which a variable in a held state must pass before the variable is no longer considered held.

Instructions: Specify the number of exception-free polling intervals. The lower the number you select, the more likely the agent is to generate repetitive event messages for a variable that is intermittently exceeding thresholds.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.15

Parameter: **Threshold Label**

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: ASN.1 OID

Options: ASN.1 OID | String identifier

Function: Specifies a name for the MIB object in string format to replace the ASN.1 object identifier. The string you enter appears in the log file, making it easier to identify the object that is the subject of the trap.

Instructions: Type a name for the MIB object, or leave this field empty to use the ASN.1 object identifier.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.22

DCM Global Parameters

Use the following guidelines to configure DCM global parameters in the Edit Base Module DCM Parameters window.

Parameter: **Enable/Disable**

Path: Configuration Manager > Platform > DCM 11.0 and later > Global ... > Base Module DCM

Default: Enable

Options: Enable | Disable

Function: Enables or disables DCMMW (the DCM software subsystem), and therefore the DCM.

Instructions: To enable the DCM, select Enable. To disable the DCM, select Disable. Use this parameter to reboot the DCM by disabling, then reenabling DCMMW.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.3

Parameter: **Boot Option**

Path: Configuration Manager > Platform > DCM 11.0 and later > Global ... > Base Module DCM

Default: Local

Options: Local | Download

Function: Specifies whether the DCM uses the image in its own Flash memory for booting or an image copied from the ANH file system to DCM shared memory (DRAM).

Instructions: Select Local to specify the image file in DCM local Flash memory as the DCM boot image. Select Download to specify an image file on the ANH Flash memory as the DCM boot image. When the DCM boots in Download mode, DCMMW software moves a copy of the image to DCM shared memory. You specify the downloaded image using the Image Name parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.8

Parameter: **Image Name**

Path: Configuration Manager > Platform > DCM 11.0 and later > Global ... > Base Module DCM

Default: None, but you must specify an image name when the Boot Option parameter is set to Download

Options: An ASCII text string, no more than 255 characters

Function: Specifies an image file on the ANH Flash memory file system as the boot image.

Instructions: Enter the volume and file name for the image that you want the DCM to boot, using the format <*volume_number:filename*>: for example, **1:dcm_image**.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.7

Parameter: Image Save Mode

Path: Configuration Manager > Platform > DCM 11.0 and later > Global... > Base Module DCM

Default: Save

Options: Save | No Save

Function: Specifies whether the DCM saves the active image in its local Flash memory or keeps the image in shared DRAM only.

Instructions: To save the DCM boot image file to the DCM local Flash memory (writing over the existing saved image), select Save. Select the No Save option if you do not want to save the DCM boot image file. (The image remains in DRAM until the next time the DCM boots.)

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.9

Parameter: Configuration Mode

Path: Configuration Manager > Platform > DCM 11.0 and later > Global... > Base Module DCM

Default: Local

Options: Local | Shared Memory

Function: Specifies whether to use configuration information in the DCM Flash memory or in the DCM shared memory space (DRAM).

Instructions: Select Local to use the default configuration information in the DCM local Flash memory. Select Shared Memory to use the configuration information in the DCM DRAM, written by DCMMW from the ANH file system.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.10

Parameter: Save Configuration Info

Path: Configuration Manager > Platform > DCM 11.0 and later > Global... > Base Module DCM

Default: Save

Options: Save | No Save

Function: Specifies whether or not to save the configuration information in DRAM to the DCM Flash memory.

Instructions: Select Save to save the configuration information in DRAM to the DCM Flash memory (writing over the existing configuration file). Select No Save to avoid overwriting the DCM configuration file.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.11

Parameter: RMON Max Host

Path: Configuration Manager > Platform > DCM 11.0 and later > Global... > Base Module DCM

Default: 500

Options: 100 to 8128

Function: Relates to the RMON Host group. Indicates the maximum number of host addresses to be collected in each entry of the RMON host control table. The maximum limit depends on the amount of Flash memory available in the DCM. When the host control table reaches the maximum value, the DCM deletes entries based on an LRU (least recently used) algorithm.

Instructions: Recommended values, based on DCM memory configurations, are

-- 2 to 4 MB: 2048
-- 3 MB: 4096
-- 16 MB: 8128

To verify the number of hosts configured, check the MIB object wfDCMmwRMONHost using the Site Manager Statistics tool.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.12

Parameter: RMON Default Host

Path: Configuration Manager > Platform > DCM 11.0 and later > Global... > Base Module DCM

Default: Enable

Options: Enable | Disable

Function: Specifies whether or not to create the RMON host control table at every boot. Some RMON network management applications expect the DCM to set up a host configuration. Others enable and disable their own configurations during normal operations.

Note that the DCM allows only one instance of the host control table.

Instructions: Select Enable to create the RMON host control table at the next (and every subsequent) reboot. Select Disable to disable default creation of the RMON host control table at boot time.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.13

Parameter: RMON Default Matrix

Path: Configuration Manager > Platform > DCM 11.0 and later > Global... > Base Module DCM

Default: Enable

Options: Enable | Disable

Function: Relates to the RMON Matrix group. Specifies whether or not to create the RMON matrix control table at every boot. Some RMON network management applications expect the DCM to set up a Matrix configuration. Others enable and disable their own configurations during normal operations.

Instructions: Select Enable to create the RMON matrix control table at the next (and every subsequent) reboot. Select Disable to disable default creation of the RMON matrix control table at boot time.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.14

BOOTP and DHCP Parameters

Use the following guidelines to configure BOOTP and DHCP parameters in the BOOTP Relay Agent Interface Table window.

BOOTP Relay Agent Interface Parameters

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: Enable

Options: Enable | Disable

Function: Specifies whether BOOTP is active on the network interface.

Instructions: Select Enable to enable BOOTP on the network interface; select Disable to disable BOOTP on the network interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.2

Parameter: Hops

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: 4

Options: 1 to 16 hops

Function: Specifies the maximum number of hops from the client to the server. A hop is the logical distance between two devices. If the value in the hops field of a BOOTREQUEST packet is greater than the number you specify for this parameter, the router drops the packet.

Instructions: Accept the default of 4 hops or specify a number from 1 to 16.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.5

Parameter: **Timeout Secs.**

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: 0

Options: 0 to 65535 seconds

Function: Specifies the minimum number of seconds that the router waits before forwarding a BOOTREQUEST packet. If the value in the seconds field of a BOOTREQUEST packet is less than the value you specify for this parameter, the router drops the packet.

Instructions: Accept the default, 0, or specify a number from 1 to 65535.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.6

Parameter: **Pass Through Mode**

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: BOOTP

Options: BOOTP │ DHCP │ BOOTP and DHCP

Function: Specifies whether the interface relays BOOTP, DHCP, or both BOOTP and DHCP requests.

Instructions: Select BOOTP to relay BOOTP requests; select DHCP to relay DHCP requests; select BOOTP and DHCP to relay both kinds of requests.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.16

BOOTP Address Parameters

Use the following guidelines to configure BOOTP and DHCP parameters in the BOOTP Addresses window.

Parameter: Input IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F > Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP interface that receives BOOTREQUEST packets from clients.

Instructions: Enter the IP address of a numbered network interface that you want to receive BOOTREQUEST or DHCP packets from clients, then configure this IP address on the router, if you have not already done so.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.3

Parameter: Output IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F > Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP interface that forwards BOOTREQUEST packets to an external network.

Instructions: Enter the IP address of a numbered network interface that you want to send BOOTREQUEST or DHCP packets to servers, then configure this IP address on the router, if you have not already done so.

Do not specify an unnumbered interface for this parameter. If you want to use an unnumbered interface to send BOOTREQUEST or DHCP packets to servers, you must set up a preferred server from the BOOTP Relay Agent Interface Table window.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.4

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F > Add**

Default: Enable

Options: Enable │ Disable

Function: Specifies whether this forwarding route is active.

Instructions: Select Enable to allow BOOTP or DHCP forwarding through this route; select Disable to prevent BOOTP or DHCP forwarding through this route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.2

Parameter: Pass Through Mode

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F > Add**

Default: BOOTP

Options: BOOTP │ DHCP │ BOOTP and DHCP

Function: Specifies whether the interface relays BOOTP, DHCP, or both BOOTP and DHCP requests.

Instructions: Select BOOTP to relay BOOTP requests; select DHCP to relay DHCP requests; select BOOTP and DHCP to relay both kinds of requests.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.5

BOOTP Client Interface Address Parameters

Use the following guidelines to configure BOOTP and DHCP parameters in the BOOTP Client Interface window.

Parameter: IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Client I/F > Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP address of the remote AN that will boot using EZ-Install over a Frame Relay group access PVC connection to the router.

Instructions: Enter the IP address of the remote AN.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.1.1.1.3

Parameter: DLCI Number

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Client I/F > Add**

Default: None

Options: 16 to 1007

Function: Specifies the Frame Relay PVC identification number whose destination is the remote AN that will boot using EZ-Install. The Frame Relay network uses the DLCI number to direct data flow.

Instructions: Enter the DLCI number, in decimal format, for the group access PVC to the remote AN. Use the DLCI number assigned by your Frame Relay service provider.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.1.1.1.2

BOOTP Preferred Server Configuration Parameters

Use the following guidelines to configure BOOTP and DHCP preferred server configuration parameters.

Parameter: Relay Agent IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP interface that receives BOOTREQUEST packets from clients.

Instructions: Enter the IP address of a numbered network interface that you want to receive BOOTREQUEST or DHCP packets from clients, then configure this IP address on the router, if you have not already done so.

Do not specify an unnumbered interface for this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.3

Parameter: Target Server IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: None

Options: Any valid IP address

Function: Specifies the address of a server that should receive BOOTREQUEST or DHCP packets.

Instructions: Enter the IP address of the server that should receive the BOOTREQUEST or DHCP packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.4

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: Enable

Options: Enable | Disable

Function: Specifies whether the forwarding route is active.

Instructions: Select Enable to allow BOOTP or DHCP forwarding through this route; select Disable to prevent BOOTP or DHCP forwarding through this route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.2

Parameter: Target Name

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: None

Options: Any string of printable ASCII characters, up to 63 characters in length, including embedded spaces

Function: Specifies the target server's host name.

Instructions: If you want to keep track of the names of BOOTP or DHCP servers, enter the target server's host name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.5

Parameter: Pass Through Mode

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: BOOTP

Options: BOOTP | DHCP | BOOTP and DHCP

Function: Specifies whether the interface relays BOOTP, DHCP, or both BOOTP and DHCP requests.

Instructions: Select BOOTP to relay BOOTP requests; select DHCP to relay DHCP requests; select BOOTP and DHCP to relay both kinds of requests.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.6

RARP Interface Parameters

Use the following guidelines to configure RARP interface parameters in the RARP Interface Table window.

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > IP > Reverse ARP > Interface Table
Default: Enable
Options: Enable | Disable
Function: Reenable or disable the RARP interface you selected from the list of interfaces.
Instructions: Select Enable to reenable a disabled interface. Select Disable to disable an interface.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.9.3.1.2

RARP Address Parameters

Use the following guidelines to configure RARP address parameters in the RARP Addresses window.

Parameter: MAC Address

Path: Configuration Manager > Protocols > IP > Reverse ARP > Map Table > **Add**
Default: None
Options: Any valid MAC address
Function: Specifies the MAC address of a client that will use the RARP services of this router.
Instructions: Enter the MAC address of a client.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.9.2.1.2

Parameter:	**IP Address**
Path:	Configuration Manager > Protocols > IP > Reverse ARP > Map Table > **Add**
Default:	0.0.0.0
Options:	Any valid IP address
Function:	Specifies the corresponding IP address for the client with the MAC address you specified using the MAC Address parameter. When the router receives a RARP request from the client, the router assigns this IP address to the client and includes it in a response packet.
Instructions:	Enter the IP address corresponding to the value of the MAC Address parameter. Do not accept the default value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.9.2.1.3

Appendix B
Default Parameter Settings

SNMP Parameters

Tables B-1 through B-4 list the Site Manager default parameter settings for SNMP.

Table B-1. SNMP Global Parameters

Parameter	Default
Enable	Enable
Use Lock	Enable
Lock TimeOut	2 minutes
Authentication Failure Traps	Enable

Table B-2. SNMP Community Parameters

Parameter	Default
Community Name	None
Access	Read Only

Table B-3. SNMP Manager Parameters

Parameter	Default
Trap Port	162
Trap Types	Generic

Table B-4. SNMP Trap Interface Parameters

Parameter	Default
Entity Code	None
Event Code	None
Always/Never Trap	None

Table B-5. SNMP Threshold Global Parameters

Parameter	Default
Enable/Disable	Enable
Polling Interval	60 seconds

Table B-6. SNMP Threshold Interface Parameters

Parameter	Default
Threshold Enable	Enable
Threshold Low Value	0
Threshold Low Event Level	Info
Threshold Medium Value	0
Threshold Medium Event Level	Info

(continued)

Table B-6. SNMP Threshold Interface Parameters *(continued)*

Parameter	Default
Threshold High Value	0
Threshold High Event Level	Info
Threshold Units	Persecond
Threshold Action	Greaterthan
Threshold Max Successive Alarms	5
Threshold HoldDown Intervals	1
Threshold Label	ASN.1 OID

DCM Global Parameters

Table B-7 lists the Site Manager default parameter settings for the DCM.

Table B-7. DCM Global Parameters

Parameter	Default
Enable/Disable	Enable
Boot Option	Local
Image Name	None
Image Save Mode	Save
Configuration Mode	Local
Save Configuration Info	Save
RMON Max Host	500
RMON Default Host	Enable
RMON Default Matrix	Enable

BOOTP and DHCP Parameters

Tables B-8 through B-11 list the Site Manager default parameter settings for BOOTP and DHCP.

Table B-8. BOOTP Relay Agent Interface Parameters

Parameter	Default
Enable/Disable	Enable
Hops	4
Timeout Secs.	0 seconds
Pass Through Mode	BOOTP

Table B-9. BOOTP Address Parameters

Parameter	Default
Input IP Address	None
Output IP Address	None
Enable/Disable	Enable
Pass Through Mode	BOOTP

Table B-10. BOOTP Client Interface Address Parameters

Parameter	Default
IP Address	None
DLCI Number	None

Table B-11. BOOTP Preferred Server Configuration Parameters

Parameter	Default
Relay Agent IP Address	None
Target Server IP Address	None
Enable/Disable	Enable
Target Name	None
Pass Through Mode	BOOTP

RARP Parameters

Tables B-12 and B-13 list the Site Manager default parameter settings for RARP.

Table B-12. RARP Interface Parameters

Parameter	Default
Enable/Disable	Enable

Table B-13. RARP Address Parameters

Parameter	Default
MAC Address	None
IP Address	0.0.0.0

Index

A

adding an SNMP manager, 3-5

B

Bay Networks
  publications, ordering, xviii

BOOTP
  client interface table, creating, 5-7
  configuring preferred servers, 5-8
  customizing relay agent parameters, 5-1
  deleting IP interface input and output address pair, 5-6
  enabling on an interface, 1-5
  filtering packets, 5-9
  overview, 2-24
  relay agent, 2-25, 2-32, 5-5
  relay agent forwarding table, 5-5
  route forwarding, 5-6
  setting up routing paths between BOOTP server and router, 5-3
  specifying IP interface input/output address pair, 5-5

BOOTP parameters
  defaults, B-4 to B-5

Bootstrap protocol. *See* BOOTP

C

Capture group, 2-15, 2-22

communities (SNMP)
  access privileges, 2-4
  configuring, 3-3
  names, 2-4

CompuServe, Bay Networks forum on, xxii

configuring
  DHCP parameters, 6-1
  SNMP community parameters, 3-3
  SNMP managers, 3-5
  SNMP trap exceptions, 3-9
  SNMP traps, 3-7
  SNMP thresholds, 3-10

Customer Service FTP, xxi

customer support, xix

customer support programs, xx

customizing
  BOOTP relay agent parameters, 5-1
  DCM parameters, 4-2
  DHCP parameters, 6-1
  RARP parameters, 7-1
  SNMP global parameters, 3-1

D

data collection module middleware (DCMMW), 2-12

DCM
  boot image, 4-2
  customizing parameters, 4-2 to 4-5

defaults
  for BOOTP and DHCP parameters, B-4 to B-5
  for DCM global parameters, B-3
  for RARP parameters, B-5
  for SNMP parameters, B-1

deleting
  BOOTP globally, 5-10
  DCMMW software, 4-5
  DHCP globally, 6-2

trap exceptions, 3-10
RARP services, 7-3
SNMP managers, 3-7

DHCP
customizing parameters, 6-1
deleting from an IP interface, 6-2
deleting globally, 6-2
enabling on an interface, 1-6
overview, 2-29
packets, 2-32 to 2-34
servers, 2-29
specifying servers for, 6-2
starting, 1-6

DHCP parameters
defaults, B-4 to B-5

disabling globally
RARP, 7-3

Dynamic Host Configuration Protocol. *See* DHCP

E

Enable/Disable parameter
for RARP, 7-3

enabling
IP services, 1-2
SNMP services, 1-2

Statistics group, 2-13

event messages, 2-5
format, 2-9
protocol entities, 2-5
severity levels, 2-6

exceptions
deleting, 3-10

F

Filter group, 2-14, 2-22

H

History group, 2-14, 2-20

Host group, 2-14, 2-20

HostTopN group, 2-14, 2-21

I

implementation notes
for SNMP, 2-4 to 2-9

InfoFACTS service, xxiii

interoperability issues for RMON, 2-18 to 2-23

IP
customizing, 1-3
enabling on an interface, 1-2
starting, 1-2

M

managers, for SNMP
adding, 3-5
deleting, 3-7

Matrix group, 2-14, 2-22

memory use
for configuring thresholds, 2-9
for RMON, 2-18 to 2-23

P

packets
BOOTP, 2-24 to 2-28
DHCP, 2-32 to 2-34

parameters
See BOOTP parameters
See RARP parameters
See SNMP parameters

R

RARP
customizing parameters, 7-1
defining the mapping table for, 7-2
deleting globally, 7-3
disabling globally, 7-3
disabling interfaces, 7-1
enabling on an interface, 1-7

overview, 2-35
reenabling interfaces, 7-1

RARP parameters
defaults, B-5
Enable/Disable, 7-3

RARP services
starting, 1-7

Request for Comments 1757, 2-11, 2-13

Reverse Address Resolution Protocol. *See* RARP

RMON
agent, 2-11
architecture, 2-12
configuring, 2-10
control parameters, 2-13
control tables, 2-13
data tables, 2-13
groups, 2-11 to 2-15
interoperability issues, 2-18 to 2-23
memory use, 2-18 to 2-23
overview, 2-10
starting, 1-3
using Optivity Analysis, 2-10
using Optivity LAN, 2-10

RMON architecture
BayStack AN and ANH base module, 2-12
DCM, 2-12
DCMMW, 2-12

S

Simple Network Management Protocol
See SNMP

SNMP
adding a community, 3-3
agents, 2-1
applications, 2-1
community, 2-4
community managers, 3-5
customizing global parameters, 3-1
deleting a community, 3-4
enabling, 1-2
events, 2-5
implementation notes, 2-4
messages
GetNextRequest, 2-2
GetRequest, 2-2
SetRequest, 2-2
network elements, 2-1
network management station, 2-1
overview, 2-1
security, 2-4
traps, 2-2, 2-5

SNMP parameters
defaults, B-1
threshold interface
Threshold Action, A-12
Threshold High Event Level, A-11
Threshold High Value, A-11
Threshold Label, A-14
Threshold Low Event Level, A-9
Threshold Low Value, A-9
Threshold Max Successive Alarms, A-13
Threshold Medium Event Level, A-10
Threshold Medium Value, A-10
Threshold Units, A-12

SNMP thresholds
configuring, 3-10

specifying. *See* configuring

starting
BOOTP services, 1-5
DHCP, 1-6
IP, 1-2
RARP services, 1-7

Support Source CD, xxii

T

Technical Response Centers, xxiii

technical support, xix

Threshold Action parameter, A-12

Threshold High Event Level parameter, A-11

Threshold High Value parameter, A-11

Threshold Label parameter, 2-9, A-14

Threshold Low Event Level parameter, A-9
Threshold Low Value parameter, A-9
Threshold Max Successive Alarms parameter, A-13
Threshold Medium Event Level parameter, A-10
Threshold Medium Value parameter, A-10
threshold polling interval, 3-11
Threshold Units parameter, A-12
thresholds
  adding, 3-11
  defining state of, 2-9
  definition, 2-7
  enabling, 3-10
  memory considerations, 2-9
  severity levels, 2-8
trap messages, 2-5
  format, 2-6
  severity levels, 2-6
traps, 2-2
  configuring, 3-7 to 3-10
  exceptions, 3-9

U

unnumbered interfaces, using for BOOTP and DHCP services, 5-8

W

World Wide Web, Bay Networks home page on, xxi